目　录

历史介绍 ……………………………………………… (1)

第一章　算术基本定理 ……………………………… (17)

1.1　引言 ……………………………………………… (17)

1.2　整除性 …………………………………………… (18)

1.3　最大公约数 ……………………………………… (19)

1.4　素数 ……………………………………………… (21)

1.5　算术基本定理 …………………………………… (22)

1.6　素数倒数的级数 ………………………………… (24)

1.7　Euclid算法 ……………………………………… (25)

1.8　两个以上的数的最大公约数 …………………… (27)

第一章习题 ……………………………………… (28)

第二章　数论函数与Dirichlet乘积 ……………… (33)

2.1　引言 ……………………………………………… (33)

2.2　Möbius函数$\mu(n)$ ……………………………… (33)

2.3　Euler函数$\varphi(n)$ ……………………………… (34)

2.4　φ与μ的相互关系 …………………………… (36)

2.5　$\varphi(n)$的一个乘积公式 ………………………… (37)

2.6　数论函数的Dirichlet乘积 ……………………… (39)

2.7　Dirichlet逆函数与Möbius反转公式 ………… (41)

2.8 Mangoldt函数$\Lambda(n)$ ………………………… (43)
2.9 积性函数 ……………………………………… (45)
2.10 积性函数与Dirichlet乘积 ………………… (46)
2.11 完全积性函数的逆函数………………………… (48)
2.12 Liouville函数$\lambda(n)$……………………… (50)
2.13 除数函数$\sigma_a(n)$ ………………………… (51)
2.14 广义卷积……………………………………… (52)
2.15 形式幂级数…………………………………… (54)
2.16 数论函数的Bell级数………………………… (57)
2.17 Bell级数与Dirichlet乘积 ………………… (58)
2.18 数论函数的导数……………………………… (59)
2.19 Selberg等式 ………………………………… (61)
第二章习题……………………………………… (61)
第三章 数论函数的平均值 ……………………… (69)
3.1 引言 …………………………………………… (69)
3.2 大O符号，函数的渐近等式 ………………… (70)
3.3 Euler求和公式 ……………………………… (71)
3.4 几个基本渐近公式 …………………………… (73)
3.5 $d(n)$的平均阶 ……………………………… (75)
3.6 除数函数$\sigma_a(n)$的平均阶 ……………… (79)
3.7 $\varphi(n)$的平均阶……………………………… (81)
3.8 对于由原点可见的格点分布的应用 ………… (82)
3.9 $\mu(n)$与$\Lambda(n)$的平均阶 ………………… (85)
3.10 Dirichlet乘积的部分和 …………………… (86)
3.11 对$\mu(n)$与$\Lambda(n)$的应用 ……………… (87)
3.12 Dirichlet乘积的部分和的另一个等式 …… (91)

第三章习题 ……………………………………………… (92)
第四章　素数分布的几个基本定理…………… (99)
4.1　引言…………………………………………… (99)
4.2　Chebyshev函数$\psi(x)$与$\theta(x)$ ……………… (100)
4.3　联系$\theta(x)$与$\pi(x)$的关系式 ………………… (102)
4.4　素数定理的几个等价形式……………………… (105)
4.5　$\pi(n)$与p_n的一些不等式 ……………………… (109)
4.6　Shapiro Tauberian定理……………………… (113)
4.7　Shapiro定理的应用 …………………………… (117)
4.8　部分和$\sum_{p<x}\left(\frac{1}{p}\right)$的一个渐近公式………… (119)
4.9　Möbius函数的部分和 ………………………… (121)
4.10　素数定理初等证明的简概………………… (130)
4.11　Selberg渐近公式…………………………… (131)
第四章习题 ……………………………………………… (133)
第五章　同余式 ……………………………………… (143)
5.1　同余的定义与基本性质………………………… (143)
5.2　剩余类与完全剩余系…………………………… (147)
5.3　一次同余式……………………………………… (149)
5.4　简化剩余系与Euler-Fermat定理 ……………… (152)
5.5　模p的多项式同余式，Lagrange定理 …… (154)
5.6　Lagrange定理的应用 ………………………… (155)
5.7　一次同余式组，中国剩余定理………………… (157)
5.8　中国剩余定理的应用…………………………… (159)
5.9　模是素数方幂的多项式同余式………………… (161)
5.10　交叉分类原理 ……………………………… (164)

5.11 简化剩余系的分解性 …………………… (168)
第五章习题 …………………………………… (169)
第六章 有限Abel群及其特征 ………………… (173)
6.1 定义…………………………………………… (173)
6.2 群和子群的例……………………………… (174)
6.3 群的基本性质……………………………… (174)
6.4 子群的结构………………………………… (176)
6.5 有限Abel群的特征 ……………………… (179)
6.6 特征群……………………………………… (181)
6.7 特征的正交关系式………………………… (182)
6.8 Dirichlet特征 ……………………………… (184)
6.9 含有Dirichlet特征的和 ………………… (187)
6.10 对于实的非主特征χ，$L(1,\chi)$不等于零
…………………………………………… (189)
第六章习题 …………………………………… (192)
第七章 算术级数里素数的Dirichlet定理
…………………………………………… (197)
7.1 引言………………………………………… (197)
7.2 形如$4n-1$与$4n+1$的素数的Dirichlet定理
…………………………………………… (198)
7.3 Dirichlet定理的证明方案 ……………… (199)
7.4 引理7.4的证明 ………………………… (202)
7.5 引理7.5的证明 ………………………… (204)
7.6 引理7.6的证明 ………………………… (206)
7.7 引理7.8的证明 ………………………… (206)
7.8 引理7.7的证明 ………………………… (207)

7.9 算术级数里素数的分布 …………………… (208)
第七章习题 …………………… (210)
第八章 周期数论函数与Gauss和 …………………… (213)
8.1 模k的周期函数 …………………… (213)
8.2 周期数论函数的有限Fourier级数的存在性 …………………… (214)
8.3 Ramanujan和及其推广 …………………… (217)
8.4 和$S_k(n)$的乘法性质 …………………… (220)
8.5 与Dirichlet特征相伴的Gauss和 …………………… (223)
8.6 具有非零Gauss和的Dirichlet特征 …………………… (225)
8.7 诱导模与本原特征 …………………… (226)
8.8 诱导模的进一步的性质 …………………… (228)
8.9 特征的前导子 …………………… (231)
8.10 本原特征与可分的Gauss和 …………………… (232)
8.11 Dirichlet特征的有限Fourier级数 …………………… (233)
8.12 本原特征部分和的Pólya不等式 …………………… (234)
第八章习题 …………………… (236)
第九章 二次剩余与二次互反律 …………………… (241)
9.1 二次剩余 …………………… (241)
9.2 Legendre符号及其性质 …………………… (243)
9.3 $\left(\frac{-1}{p}\right)$与$\left(\frac{2}{p}\right)$的值 …………………… (245)
9.4 Gauss引理 …………………… (247)
9.5 二次互反律 …………………… (251)
9.6 互反律的应用 …………………… (254)
9.7 Jacobi符号 …………………… (256)

9.8 对Diophantu方程的应用 …………………… (260)
9.9 Gauss和与二次互反律 ………………………… (262)
9.10 二次Gauss和的互反律 ………………………… (267)
9.11 二次互反律的另一个证明 ………………………… (274)
第九章习题 …………………………………………… (275)
第十章 原根 …………………………………………… (279)
10.1 数的次数modm，原根 ………………………… (279)
10.2 原根与简化剩余系 ………………………… (280)
10.3 对$\alpha \geqslant 3$，模2^{α}的原根不存在 ……………… (281)
10.4 对奇素数P，模P的原根存在……………… (282)
10.5 原根与二次剩余 ………………………… (284)
10.6 模p^{α}的原根存在 ………………………… (284)
10.7 模$2p^2$的原根存在 ………………………… (287)
10.8 其他情况下原根不存在 ………………………… (288)
10.9 模m的原根的个数 ………………………… (289)
10.10 指数的计算………………………………… (291)
10.11 原根与Dirichlet特征 ………………………… (296)
10.12 模p^{α}的实值Dirichlet特征 ……………… (299)
10.13 模p^{α}的本原Dirichlet特征 ……………… (300)
第十章习题 …………………………………………… (302)
第十一章 Dirichlet级数与Euler乘积 ……… (307)
11.1 引言 …………………………………………… (307)
11.2 Dirichlet级数绝对收敛的半平面 ………… (308)
11.3 由Dirichlet级数定义的函数……………… (309)
11.4 Dirichlet级数的乘积………………………… (312)
11.5 Euler乘积 ………………………………… (314)

11.6 Dirichlet级数收敛的半平面 …………………(317)
11.7 Dirichlet级数的解析性质 ……………………(320)
11.8 具有非负系数的Dirichlet级数 ………………(323)
11.9 Dirichlet级数表示为Dirichlet级数的指数 ……………………………………………………(325)
11.10 Dirichlet级数的平均值公式 ……………(328)
11.11 Dirichlet级数系数的一个积分公式 ……(331)
11.12 Dirichlet级数部分和的一个积分公式 ……………………………………………………(332)
第十一章习题 ……………………………………………(338)
第十二章 函数$\zeta(s)$与$L(s, \chi)$ ……………………(343)
12.1 引言 ……………………………………………(343)
12.2 gamma函数的性质 ……………………………(344)
12.3 Hurwitz zeta函数的积分表示 ……………(345)
12.4 Hurwitz zeta函数的围道积分表示 ………(348)
12.5 Hurwitz zeta函数的解析开拓 ……………(351)
12.6 $\zeta(s)$与$L(s, \chi)$的解析开拓 ……………(352)
12.7 $\zeta(s, a)$的Hurwitz公式 …………………(353)
12.8 Riemann zeta函数的函数方程 ……………(357)
12.9 Hurwitz zeta函数的函数方程 ……………(359)
12.10 L-函数的函数方程 ………………………(361)
12.11 求$\zeta(-n, a)$的值 …………………………(364)
12.12 Bernoulli数与Bernoulli多项式的性质 ……………………………………………………(366)
12.13 $L(0, \chi)$的公式 ……………………………(369)
12.14 用有限和逼近$\zeta(s, a)$ ……………………(370)

12.15　$|\zeta(s, a)|$的不等式 ………………………… (373)
12.16　$|\zeta(s)|$与$|L(s, \chi)|$的不等式 …………… (376)
第十二章习题 ……………………………………… (377)
第十三章　素数定理的解析证明 ……………… (385)
13.1　证明的方案 ……………………………………… (385)
13.2　引理 ……………………………………………… (387)
13.3　$\frac{\Psi_1(x)}{x^2}$的围道积分表示 ………………… (391)
13.4　直线$\sigma=1$附近$|\zeta(s)|$与$|\zeta'(s)|$的上界…… (394)
13.5　在直线$\sigma=1$上$\zeta(s)$不为零 ………………… (396)
13.6　$\left|\frac{1}{\zeta(s)}\right|$与$\left|\frac{\zeta'(s)}{\zeta(s)}\right|$的不等式 …………… (398)
13.7　素数定理证明的完成 ………………………… (400)
13.8　$\zeta(s)$的无零点区域 ………………………… (403)
13.9　Riemann假设 ………………………………… (406)
13.10　对除数函数的应用………………………… (407)
13.11　对Euler函数的应用 ……………………… (412)
13.12　特征和的Pólya不等式的推广…………… (416)
第十三章习题 ……………………………………… (417)
第十四章　分拆 ……………………………………… (423)
14.1　引言 ……………………………………………… (423)
14.2　分拆的几何表示 ……………………………… (427)
14.3　分拆的生成函数 ……………………………… (427)
14.4　Euler五边形数定理 ………………………… (431)
14.5　Euler五边形数定理的组合证明 ………… (435)
14.6　$P(n)$的Euler递推公式 ……………………… (438)

14.7 P(n)的上界 ……………………………………（439）
14.8 Jacobi三重积等式 ……………………………（442）
14.9 Jacobi等式的推论 ……………………………（445）
14.10 生成函数的对数微分……………………………（446）
14.11 Ramanujan的分拆等式 ………………………（449）
第十四章习题 ……………………………………（450）
参考文献目录 ……………………………………………（457）
特殊符号索引 ……………………………………………（469）

历 史 介 绍

数论是数学的一个分枝，它研究整数的性质，

1，2，3，4，5，…

叫做计数数，或者正整数。

正整数无疑是人类的第一个数学创造，假如人们没有计数的能力，那简直是很难想象的，至少在一个有限的范围内。历史的记载证明，早在公元前5700年，古代的沙麦朗(Sumerina)人就有一部历书，所以他们一定掌握了一些算术知识。

公元前2500年沙麦朗人产生了一个以60为基的数系，他们早于巴比伦人成为有熟练计算能力的人。巴比伦人的墓碑中发现有精心制作的数学表格，其日期可追溯至公元前2000年。

当古代文化发展到一定水平时，人们有空闲时间去思考周围的事物，一些人开始去探索周围自然界与数的性质，这种好奇心发展为数字神秘主义或者数字学。甚至在今天，比如3、7、11和13这些数字仍是考虑运气好或坏的予兆。

系统地研究数以前至少有5000年，数字是用于保存记录和商业交往。第一个科学地对整数进行研究，即数论的真正起源，通常认为是希腊人。大约在公元前600年，毕达哥拉斯

(Pythagoras)和他的门徒们对整数做过较彻底的研究，他们最早以各种方法对整数进行分类：

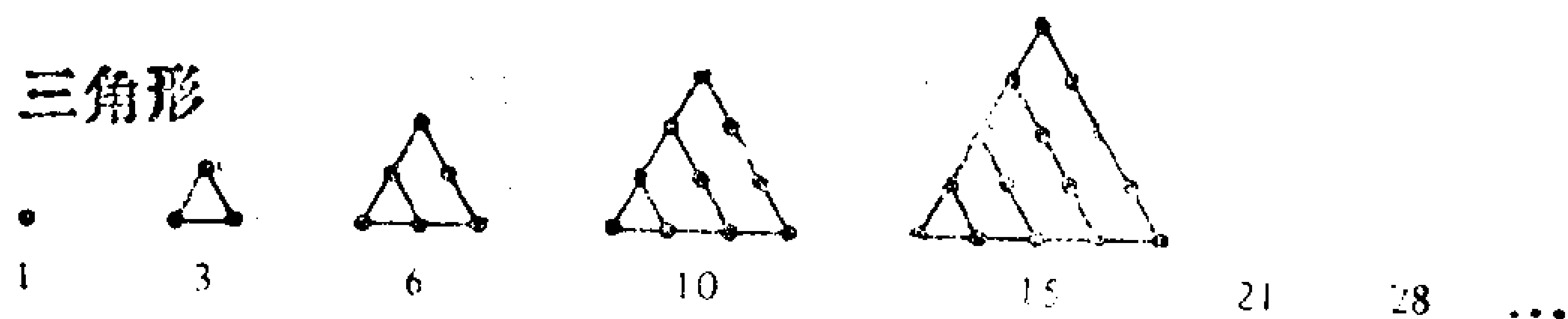
偶数：2，4，6，8，10，12，14，…

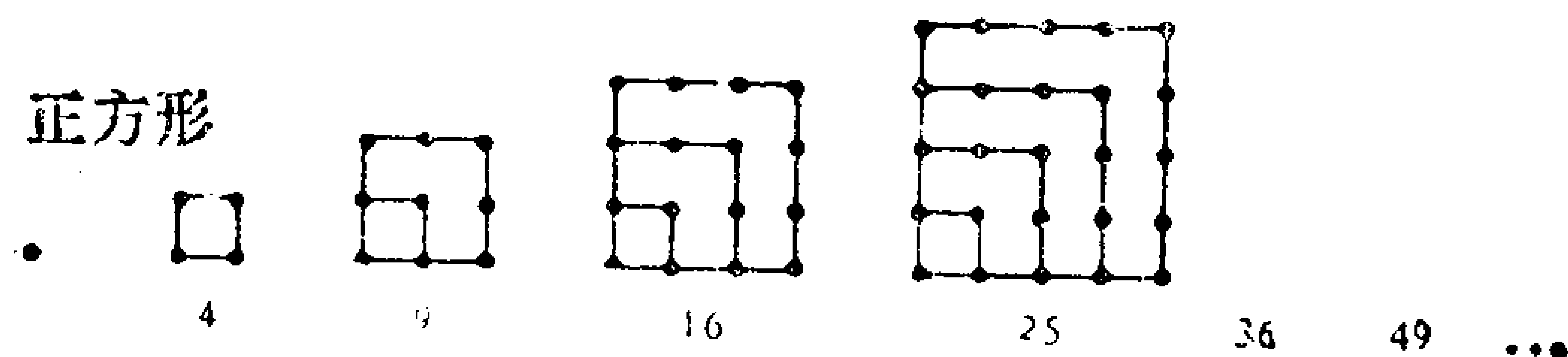
奇数：1，3，5，7，9，11，13，15，…

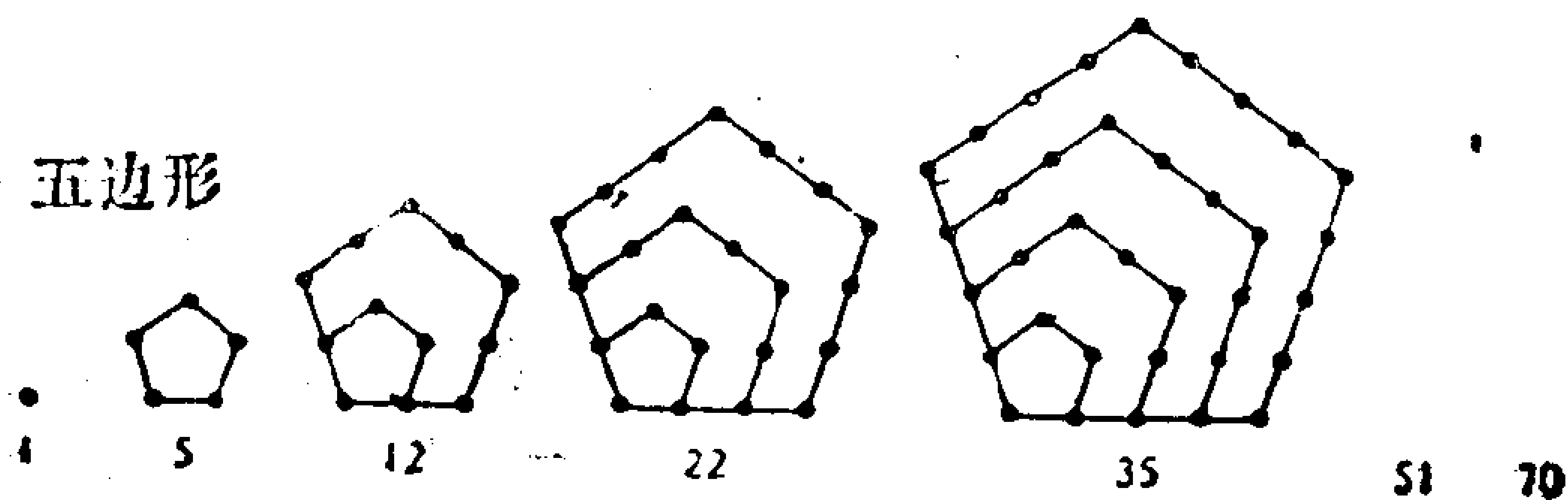
素数：2，3，5，7，11，13，17，19，23，29，31，37，41，43，47，53，59，61，67，71，73，79，83，89，97，…

复合数：4，6，8，9，10，12，14，15，16，18，20，….

素数是仅有约数1和自身的大于1的整数．除去1既不是素数也不是复合数以外，不是素数的整数称为复合数．



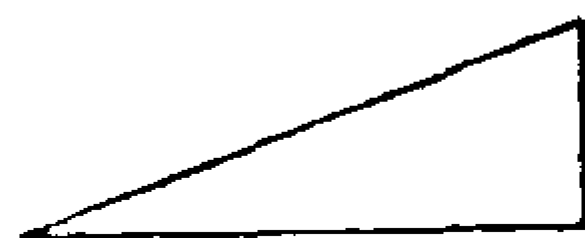




(图1.1)

Pythagoras还把数与几何图形联系起来，他创建了多边形数的思想：三角形数，正方形数，五边形数，等等．当然用三角形，正方形，五边形等图形上的点表示数时，这些几何名称的由来是显然的，如图1.1所示．

另一个与几何图形的联系来自著名的Pythagoras定理（我国称为勾股定理——译者），它说明，在任何一个直角三角形里，斜边长的平方是两直角边长的平方和（参看图1.2）．Pythagoras感兴趣的是边长都是整数的直角三角形，如图1.3那样的三角形现在称为Pythagoras三角形，对应的表示边长的三个数(x，y，z)称为Pythagoras三数组．



（图1.2）

由大约在公元前1700年的巴比伦墓碑中发现有Pythagoras的一个大表格，其中一些数字相当的大．Pythagoras第一个给出了确定无穷多个三数组的方法，用现代的记号可表述如下：

令n是任一大于1的奇数，并令

$$x=n,\quad y=\frac{1}{2}(n^2-1),\quad z=\frac{1}{2}(n^2+1).$$

这样产生的三数组(x，y，z)始终是$z=y+1$的Pythagoras三数组，下面有一些例子：

x	3	5	7	9	11	13	15	17	19
y	4	12	24	40	60	84	112	144	180
z	5	13	25	41	61	85	113	145	181

此外，还有其他一些Pythagoras三数组，例如：

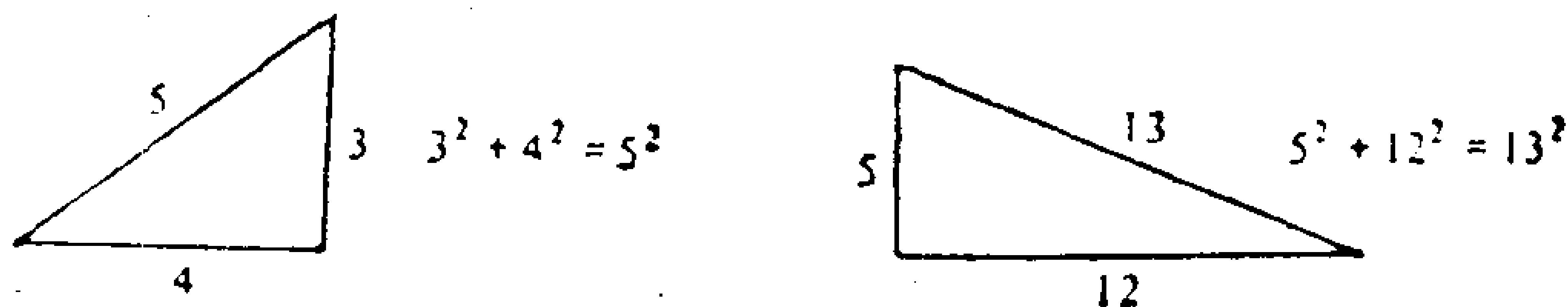
x	8	12	16	20
y	15	35	63	99

z　17　37　65　101

在这些例子里，$z=y+2$. Plato（公元前430—349年）发现了一个确定所有这些三数组的方法，用现代的记号可写为公式：

$$x=4n,\ y=4n^2-1,\ z=4n^2+1.$$

大约在公元前300年，在数学史上发生一件重大事件，Euclid基本原理、一个包含有13卷书的书集发表了，它把数学由数字学转变为演绎推理学. Enclid是第一个把数学事实和这些事实的严格证明一起给出的人.



（图1.3）

13卷书中有3卷是专门介绍数论的（卷Ⅶ、Ⅸ和Ⅹ）. 在卷Ⅸ里Euclid证明了有无穷多个素数存在. 他的证明在现代的课堂里仍在讲授. 在卷Ⅹ里 他给出了得到全部Pythagoras三数组的一个方法，虽然他没有给出他的方法的任何证明. 这个方法可概括为公式

$$x=t(a^2-b^2),\ y=2tab,\ z=t(a^2+b^2),$$

其中t，a和b是任意正整数，满足$a>b$，a与b互素，a与b一奇一偶.

Euclid还对Pythagoras提出的另一个问题——找出所有的完全数作出了重要贡献. 数6叫做一个完全数，因为$6=1+2+3$，即6等于它的所有的真因子的和（即所有小于6的因数的和）. 另一个完全数是28，因为$28=1+2+4+7$

+14，而1，2，4，7和14是28的所有小于28的因数．希腊人把一个数的真因数统称为它的“部分”，他们把6和28称为完全数，因为每个这样的数等于它的全部的“部分”的和．

在卷Ⅸ里，Euclid发现了所有的偶完全数．他证明，一个偶数如果有形式

$$2^{p-1}(2^p-1),$$

则这个偶数一定是完全数，其中P和2^p-1都是素数．

两千年以后Euler证明了Euclid定理的逆定理，即每一个偶完全数一定有Euclid形式．例如，对于6和28，我们有

$$6=2^{2-1}(2^2-1)=2\cdot 3,\quad 28=2^{3-1}(2^3-1)=4\cdot 7.$$

最前面的5个偶完全数是

6，28，496，8128和33550336。

实际上，完全数是很稀少的，迄今（1975年）只知道24个完全数，它们在Euclid形式中对应着的P的值如下：

2，3，5，7，13，17，19，31，61，89，107，127，521，607，1279，2203，2281，3217，4253，4423，9689，9941，11213，19937．

形如2^p-1的数（其中p是素数）称为Mersenne数，记为M_p，这是为了记念Mersenne，他在1644年研究了这些数．对于上面表中所列的24个素数p，已经知道M_p都是素数，而对于其他所有的$p\leqslant 257$，除去可能的

$$p=157,\ 167,\ 193,\ 199,\ 227,\ 229$$

之外，M_p是复合数．而对这几个p，还不知道M_p是素数或者是复合数．

不知道是否有奇完全数，甚至任何一个的存在性也不知

道．但如果存在的话，它一定是很大的，实际上要大于10^{50}（参看文献[29]）．

现在我们转向从Euclid时代以来数论历史的简短的描述．

在公元前300年Euclid以后，到公元250年另一个希腊数学家，阿历山得鲁的Diophantu以前，在数论方面没有重大进展，Diophantu出版过13本书，其中6本保存下来．这是第一个系统地利用代数符号的希腊人的工作，虽然他的代数符号用现代的标准来衡量好象是笨拙的，但Diophantu的方法确实能解含有两个或三个未知量的代数方程．他的许多问题来源于数论并且自然地去找这些方程的整数解．未知量具有整数解的方程现在称为Diophantu方程，而这些方程的研究就是著名的Diophantu解析．Pythagoras三数组的方程$x^2+y^2=z^2$就是Diophantu方程的一个例子．

Diophantu之后，直到17世纪，尽管在远东，——尤其在印度——在公元500年至公元1200年这段时间出现数论开始繁荣的证据，但在数论方没有出现更多的进展．

17世纪，在西欧，数论复兴．由于卓越的法国数学家Fermat（1601—1665）作出大量的成果，他被公认为近代数论的奠基人．Fermat的大多数成果是受Diophantu工作的影响而得的．他第一个真正深刻地揭示出整数的性质．例如，Fermat证明了下列令人惊奇的定理：

每一个整数不是一个三角形数就是2或3个三角形数之和；每一个整数不是一个平方数就是2、3或4个平方数之和；每一个整数不是一个五边形数就是2，3，4或5个五边形数之和，等等．

Fermat还发现，每一个形如$4n+1$的数，比如5，13，17，29，37，41等等，是两个平方数之和，例如，

$5=1^2+2^2$，$13=2^2+3^2$，$17=1^2+4^2$，

$29=2^2+5^2$，$37=1^2+6^2$，$41=4^2+5^2$.

Fermat时代之后不久，在数论的深入发展方面，Euler（1703—1783）、Lagrange（1736—1813）、Legendre（1752—1833）、Gauss（1777—1855）和Dirichlet（1805—1859）成为突出的名字．第一本数论教科书在1798年由Legendre发表，三年以后Gauss发表了数论专题论文，把论题变为系统的和美妙的学科的一本书．虽然他对数学的其他分枝和其他学科作出了巨大的贡献，而Gauss本人认为他的数论书是他的最巨大的工作．

Gauss时代以后的大约一百年里，在不同的方向上，数论有了迅速的进展．在少数的几页里要给出数论研究这类问题的清楚的断面是不可能的．这个领域是广阔的并且一些部分需要高等数学高深的学问．不过数论里有很多问题是很容易阐明的，这些问题中的一些涉及素数，我们把这个历史介绍的余下部分专门用于这些问题．

在前面有一个小于100的素数表．小于一千万的素数表由一个美国数学家D.N.Lehmer[43]在1914年发表．小于一千万的素数有664579个，大约有$6\frac{1}{2}\%$的误差，更近一些，D.H.Lehmer[D.N.Lehmer的儿子]计算出小于100亿的素数总数有455052512个，大约有$4\frac{1}{2}\%$的误差，虽然所有这些素数的每一个并不一定知道（参看Lehmer[41]）．

素数表的仔细的观察展示出，素数是以很不规则的方式

分布的．素数表显现出素数之间可以有很长的间隔，例如，素数370261后面紧着111个复合数，在20831323与20831533之间没有素数．容易证明，素数之间任意大的间隔都是能够出现的．

另一方面，素数表也指出，相邻（连续）素数，例如3和5，或101和103，总会重新出现．差数为2的素数对就是著名的孪生素数．100000以内的孪生素数超过1000对，1000000以内的孪生素数超过8000对．至今知道的最大的孪生素数对（参看William与Zarnke[76]）是$76\cdot 3^{139}-1$与$76\cdot 3^{139}+1$．很多数学家认为有无穷多个这样的素数对，但至今没有人能证明它．

素数分布不规则的原因之一是不存在产生所有素数的简单的公式．一些公式能产生很多素数，例如，式子

$$x^2-x+41$$

对于$x=0, 1, 2, \cdots, 40$分别给出一个素数，而

$$x^2-79x+1601$$

对于$x=0, 1, 2, \cdots, 79$也都给出素数，但是，没有这样简单的公式能对所有的x都给出素数，甚至利用三次幂和更高次幂也不行．实际上，Goldbach在1752年证明了，没有一个x的整系数多项式能对所有的x或对所有充分大的x都是素数．

某些多项式能表示无穷多个素数，例如，当x通过整数0，1，2，3，…时，一次多项式

$$2x+1$$

给出所有的奇数，因而给出无穷多个素数．又如多项式

$$4x+1与4x+3$$

的每一个都能给出无穷多个素数．在1837年发表的一篇著名的研究论文里，Dirichlet证明，如果a与b都是正整数并且是互素的，那么当x通过所有的正整数时，多项式

$$ax+b$$

给出无穷多个素数．这个结果，现在就是众所周知的关于在一个给定的算术级数里素数存在性的Dirichlet定理．

为了证明这个定理，Dirichlet超出整数的范围并引入解析的方法如极限和连续性，根据这个作法，他创建了称为解析数论的一个新的数学分枝的基础．在解析数论里，实分析与复分析的概念和方法仅限于与整数有关的问题．

不知道是否有二次多项$ax^2+bx+c(a\neq 0)$表示无穷多个素数．然而，Dirichlet[16]利用他的卓有成效的解析的方法证明了，如果a，2b与c没有公共素因子，则两个变量的二次多项式

$$ax^2+abxy+cy^2$$

当x和y通过所有正整数时，它能表示无穷多个素数．

Fermat猜想，对于$n=0, 1, 2, \cdots$，公式$2^{2^n}+1$总是给出素数．这些数称为Fermat数并记为F_n．前5个是$F^0=3$，$F_1=5$，$F_2=17$，$F_3=257$和$F_4=65,537$，它们都是素数．但在1732年Euler发现F_5是复合数．实际上，

$$F_5=2^{32}+1=641\cdot 670047.$$

这些数在平面几何里也是有趣的．Gauss证明，如果F_n是素数，$F_n=p$，那么正p边形能用圆规和直尺作出．

超过F_5，还没有发现其它的Fermat数是素数．实际上，对于$5\leqslant n\leqslant 16$，每一个Fermat数F_n都是复合数，而且对于下面更多的n的孤立的值，已经知道F_n是复合数：

n＝18，19，21，23，25，26，27，30，32，36．38，
39，42，52，55，58，63，73，77，81，117，125，
144，150，207，226，228，260，267，268，284，
316，452与1945．

已知的最大的Fermat复合数是F_{1945}，它超过10^{582}位数，这个数超过洛杉矶和纽约的电话号码簿的字母的总数（参看Robinson[59]与Wrathall[77]）．

前面谈到，没有一个简单的公式能给出所有的素数．在这个问题上，我们要谈到在1947年由美国数学家W．H．Mills[50]发现的一个结果．他证明，存在某个大于1但不是整数的数A，使得

对所有的x＝1，2，3，…，$[A^{3^x}]$是素数，其中$[A^{3^x}]$表示$\leqslant A^{3^x}$的最大整数．遗憾的是，没有人知道A等于什么．

前面说明了素数的分布是不规则的，然而，观察一大组素数发现它们的平均分布又好象是很规则的．虽然，素数没有终点，当我们在素数表上取更多更远的素数时，按平均数计算，它们的距离变得更大．素数频率减少的问题是早在十九世纪数学家们思索较多的一个题目．为了研究分布性，我们考虑一个记号为$\pi(x)$的函数，它是$\leqslant x$的素数的个数的总数，即

$$\pi(x) = \text{满足} 2 \leqslant p \leqslant x \text{的素数} p \text{的个数}.$$

下面是这个函数的一个短表，并把它与$\frac{x}{\log x}$比较，其中log是x的自然对数．

x	$\pi(x)$	$\frac{x}{\log x}$	$\frac{\pi(x)}{\frac{x}{\log x}}$
10	4	4.3	0.93
10^2	25	21.7	1.15
10^3	168	144.9	1.16
10^4	1229	1086	1.11
10^5	9592	8686	1.10
10^6	78498	72464	1.08
10^7	664579	621118	1.07
10^8	5761455	5434780	1.06
10^9	50847534	48309180	1.05
10^{10}	455052512	434294482	1.048

考察这个表中$x\leq 10^6$部分，Gauss[24]与Legendre[40]各自独立地提出，对于相当大的x，比值

$$\frac{\pi(x)}{\frac{x}{\log x}}$$

接近于1，并且他们推测，当x趋于∞时，这个比值将趋于1．Gauss与Legendre都想证明这个论断但都没有成功，确定这个猜想是正确的或是谬误的问题，最近一百年来引起了很多著名数学家的关注．

1851年俄国数学家Chebyshev[9]把这个问题向前推进了重要一步．他证明了，如果这个比趋于一个极限，那么这个极限一定是1．但他没能证明这个比趋于一个极限．

1859年Riemann[58]用解析的方法攻克这个问题，他利用了Euler在1737年发现的一个公式，对于实数$S>1$，这个

公式把素数与函数

$$\zeta(s)=\sum_{n=1}^{\infty}\frac{1}{n^s}$$

联系起来. Riemann考虑S的复数值并描绘出一个联系素数的分布与函数$\zeta(s)$的性质的巧妙方法的轮廓. 数学家们需要证明他的没有完全展示出的方法的所有细节是正确的, 而Riemann在1866年去世之前并没有完全解决这个问题.

30年后由于掌握了必需的解析的工具, 1896年J.Hadamard[28]与C.J.de la Vallée Poussin[71]分别独立地几乎是同时成功地证明了

$$\lim_{x\to\infty}\frac{\pi(x)\log x}{x}=1.$$

这个卓越的成果叫做素数定理, 它的证明是解析数论的辉煌成就之一.

1949年, 两个当代数学家Atle Selberg[62]与Paul Erdòs[19]给数学界引起一次轰动. 当时他们发现了素数定理的一个初等证明. 他们的证明, 尽管很高深, 但没有利用$\zeta(s)$, 也没有利用复变函数理论, 原则上讲, 对于任何熟悉初等微积分的人都是可以理解的.

关于素数的最著名的问题之一是所谓的Goldbach猜想. 1742年, Goldbach[26]写信给Euler认为任何$\geqslant 4$的偶数都是两个素数的和, 例如

$$4=2+2,\quad 6=3+3,\quad 8=3+5$$
$$10=3+7=5+5,\quad 12=5+7.$$

这个猜想至今没有解决, 虽然近几年的一些进展显示它可能是正确的. 在数学家们还没能证明它时, 为什么认为它可能

是正确的呢？首先，这个猜想对于所有小于33×10^6的偶数由实际计算已被证实．已经发现任何一个大于6而小于33×10^6的偶数实际上不仅是两个奇素数的和，而且是两个不同的奇素数的和（参看Shen[66]）．但是，在数论里千万件事例的验证是不足以使数学家们相信某事是真实的．例如，所有奇素数分为形如$4n+1$和$4n+3$两种类型，令$\pi_1(x)$表示形如$4n+1$的$\leqslant x$的所有素数的个数，$\pi_3(x)$表示形如$4n+3$的$\leqslant x$的所有素数的个数．两种类型的素数各有无穷多个是已知的．根据计算得到，对所有$x<26861$，$\pi_1(x)\leqslant\pi_3(x)$．但在1957年，J.Leech[39]得到，对于$x=26861$，$\pi_1(x)=1473$而$\pi_3(x)=1472$，所得不等号与前面所说相反。1914年Littlewood[49]证明了这个不等式经常无限地前后来回反向，即有无穷多个x，使$\pi_1(x)<\pi_3(x)$，也有无穷多个x，使$\pi_1(x)>\pi_3(x)$．根据成千上万次事例的计算验证过的，关于素数的猜想也可能是错误的．因此，Goldbach猜想对所有小于33×10^6的偶数验证的事实只是有利于它的很小一点证据．

数学家们收集关于猜想的特殊情形的正确性的证据的另一方法是证明其它的有些类似于猜想的定理．例如，在1930年，俄国数学家Schnirelmann[61]证明，存在一个数M，使得每一个整数n从某种意义上看是M个或更少的素数之和：

$$n=p_1+p_2+\cdots+p_m\quad（对充分大的n）．$$

如果我们知道对所有偶数n，M等于2，这将是证明对所有充分大的n，Goldbach猜想成立．1956年中国数学家尹文霖[78]证明了$M\leqslant18$，这就是说每一个整数n从某种意义上看

是18个或更少个素数的和．Schnirelmann的结果被认为是向Goldbach猜想的证明前进的一大步，它是近200年来在这个问题上作出的第一个真正的进展．

更接近于Goldbach猜想的解决是在1937年由俄国的另一位数学家I.M.Vinogradov作出的．他证明了，从某种意义上看，每一个奇数是三个素数的和：

$$n=p_1+p_2+p_3\text{（n是充分大的奇数）}.$$

实际上，对所有大于$3^{3^{15}}$的奇数n，这是正确的（参看Borodzkin[5]）．迄今，这是有利于Goldbach猜想证明的最强有力的武器．首先，容易证明Vinogradov定理是Goldbach论断的一个推论．也就是说，如果Godbach猜想是正确的，那么很容易推出Vinogradov的论述．Vinogradov的成绩巨大在于他没有利用Goldbach论断而能证明他自己的结果．遗憾的是，没有一个人能用另外的方法完成它的证明并由Vinogradov定理证明Goldbach猜想．

有利于Goldbach猜想证明的另一个证据是在1948年由匈牙利数学家Rényi[57]得到的．他证明了，存在一个数M，使得每一个充分大的偶数n能够写为一个素数与另一个素因子的个数不超过M的数之和：

$$n=p+A,$$

其中A的素因子不超过M个（n是充分大的偶数）．如果我们知道M＝1，那么Goldbach猜想对所有充分大的n是正确的．1965年A.A.Buhštab[6]与A.I.Vinogradov[72]证明M≤3，1966年陈景润证明M≤2．

我们简要地谈谈关于素数的一些著名的尚未解决的问题来结束这个介绍．

1. (Goldbach问题)是否有一个大于2的偶数，它不是两个素数的和？
2. 有没有一个大于 2 的偶数，它不是两个素数的差？
3. 有没有无穷多个孪生素数？
4. 有没有无穷多个Mersenne素数？Mersenne素数 就是形如2^p-1的素数，其中p是素数.
5. 有没有无穷多个Mersenne数是复合数？
6. 有没有无穷多个Fermat素数？Fermat素 数 就 是 形 如$2^{2^n}+1$的素数.
7. 有没有无穷多个Fermat数是复合数？
8. 有没有无穷多个形如x^2+1的素数？其中x是整数.（已经知道有无穷多个形 如 x^2+y^2，x^2+y^2+1，$x^2+y^2+z^2+1$的素数）.
9. 有没有无穷多个形如x^2+K（K是给定的）的 素数？
10. 对于每一个整数$n\geq1$，在n^2与$(n+1)^2$之间 是否总是至少存在一个素数？
11. 对于每一个整数$n>1$，在n^2与n^2+n之间是 否总是至少存在一个素数？
12. 是否有无穷多个各位数字（基数为10）全是 1 的素数？（有两 个 例子：11和11，111，111，111，111，111，111，111.）

专业数学家们被数论所吸引是因为看来现代数学的所有方法都能运用在数论的问题上. 实际上，很多重 要 的 数 学分支起源于数论. 例如，最初试图证明素数定理 促 进 了 复变函数论尤其是整函数论的发展，试图 证 明，当 $n\geq3$ 时，Diophantu方程$x^n+y^n=z^n$没有非平凡解（Fermat猜想）导

致代数数论的发展. 代数数论是现代数学研究最有活力的领域之一. 即使Fermat猜想仍未解决, 与在这个猜想上的研究工作中已经创造出的大量有价值的数学成果相比, 问题是否解决并不是很重要的. 另一个例子是分拆理论, 它已成为组合分析的发展和模函数研究中的一个重要因素.

数论中有几百个尚未解决的问题. 新问题的出现比老问题的解决更快, 并有很多几个世纪留下来的未解决的问题. 正如数学家Sierpinski曾说过的那样: "…, 我们对数的认识的进展不仅是推进关于它们我们已经知道的东西, 还要去认识关于它们我们不知道的东西."

注: 每一个认真学习数论的大学生都知道Dickson的数论历史的三卷书[13]和Le Veque的数论评论的六卷书[45]. Dickson的《历史》给出一个直到1918年为止的全部数论文献的百科大全, Le Veque的书重现了《数论评论》(1940—1972)中与数论问题直接有关的全部评论文章. 这两部珍贵的藏书实际上提供了从古代直到1972年在数论方面所有的重要发现的历史.

第一章 算术基本定理

1.1 引言

这一章介绍初等数论的基本概念，如整除性，最大公约数、素数及复合数等．主要的结果是定理1.2，它肯定了任意两个整数的最大公约数的存在性．还有定理1.10（算术基本定理），它证明了每一个大于1的整数都可以唯一地表示为素因数的乘积（不计因数的顺序）．许多证明的成立要利用到下面的整数的性质．

归纳法原理 如果Q是一个具有如下性质的集合，

(a) $1\in Q$,

(b) $n\in Q$就有$n+1\in Q$,

则

(c) 所有$\geqslant 1$的整数都属于Q.

当然，这个原理有替换的形式，例如，在(a)里，整数1可用任意整数K代替；在(c)中不等式$\geqslant 1$可换为$\geqslant K$；还有(b)可换为$1, 2, 3, \cdots, n\in Q$推出$(n+1)\in Q$.

我们假定读者对这个原理以及利用它去证明定理是熟悉的，我们也假定读者熟悉下面的原理，它与归纳法原理是逻

辑等价的.

良序原理 如果A是一个以正整数为元素的非空集合，那么A一定包含有一个最小的元素.

这个原理也有等价的形式，例如，其中的"正整数"可以用"对某个K，整数≥K"代替.

注：本章内，小写拉丁字母a，b，c，d，n等表示整数，它们可以是正的、负的或者是零.

1.2 整除性

整除的定义. 当$n=cd$时，我们说d整除n并记为$d|n$，我们也说n是d的倍数，d是n的一个约数或因数. 如果d不能整除n，我们就记为$d\nmid n$.

整除在任意两个整数之间建立了一个关系，它具有下列基本性质，其证明作为练习留给读者.

定理1.1 整除有下列性质：

(a) $n|n$ （反身性）

(b) $d|n$与$n|m$推出$d|m$ （传递性）

(c) $d|n$与$d|m$推出$d|(an+bm)$ （线性性）

(d) $d|n$推出$ad|an$ （乘法性）

(e) $ad|an$，$a\neq 0$推出$d|n$ （消去律）

(f) $1|n$ （1整除每个整数）

(g) $n|0$ （每个整数都整除零）

(h) $0|n$必有$n=0$ （零只能整除零）

(i) $d|n$，$n\neq 0$必有$|d|\leqslant|n|$

(j) $d|n$，$n|d$必有$|d|=|n|$

(k) $d|n$，$d\neq 0$，必有$\frac{n}{d}\Big|n$.

注：如果$d|n$，那么$\frac{n}{d}$叫做d的共轭因子.

1.3 最大公约数

如果d整除两个整数a与b，那么d称为a与b的公约数. 于是，1是任意一对整数a与b的公约数. 现在我们证明，任意一对整数a与b一定有一个公约数可以表示为a与b的线性组合.

定理1.2 给定任意两个整数a与b，一定存在一个形如

$$d=ax+by$$

的a与b的公约数d，这里x与y是整数，而且a与b的每一个公约数都整除这个d.

证明 首充，我们假定$a\geqslant 0$，$b\geqslant 0$，我们对n作归纳法，这里$n=a+b$. 如果$n=0$，则$a=b=0$，我们可以取$d=0$，$x=y=0$. 于是我们假设定理对0，1，2，…，$n-1$是成立的. 根据对称性，我们可以设$a\geqslant b$. 如果$b=0$，则取$d=a$，$x=1$，$y=0$. 如果$b\geqslant 1$，就对$a-b$与b用这个定理. 因为$(a-b)+b=a=n-b\leqslant n-1$，根据归纳法假设，结论是成立的，并且$a-b$与b有一个形如$d=(a-b)x+by$的公约数d. 这个d也整除$(a-b)+b=a$，所以d是a与b的一个公约数并且我们有$d=ax+(y-x)b$，这是a与b的一个线性组合. 为了完成证明我们还需要说明每一个公约数都整除d. a与b的公约数整除a与b，根据线性性也就整除d.

如果$a<0$或者$b<0$（或者两个均小于零），我们对$|a|$与$|b|$用上面的结果，于是有一个$|a|$与$|b|$的公约数 d 有形式

$$d=|a|x+|b|y,$$

如果$a<0$，则$|a|x=-ax=a(-x)$．同样，如果$b<0$，则$|b|y=b(-y)$，因此d还是a与b的一个线性组合． □

定理1.3　给定整数a与b，有且仅有一个整数d具有如下性质：

(a) $d\geqslant 0$　　　　（d是非负的）

(b) $d|a$且$d|b$　　　　（d是a与b的一个公约数）

(c) 若$e|a$，$e|b$，则$e|d$　　　　（每一个公约数都整除d）

证明　根据定理1.2，至少有一个d满足条件(b)与(c)．但若d'也满足(b)与(c)，那么$d|d'$且$d'|d$,所以$|d|=|d'|$，因此只有一个$d\geqslant 0$满足(b)与(c)． □

注：在定理1.3中，当且仅当$a=b=0$时，$d=0$，在其它情况下$d\geqslant 1$．

定义　定理1.3里的数d称为a与b的最大公约数(gcd)且用(a，b)或aDb表示．如果$(a,b)=1$，则称a与b是互素的．

记号aDb来自于把最大公约数理解为对a与b施行运算．但是最常用的记号是(a，b)，尽管在下面的定理中我们也用记号aDb，那是为强调运算D的代数性质．

定理1.4　gcd具有如下性质：

(a) $(a, b)=(b, a)$

　　$aDb=bDa$　　　　（交换律）

(b) $(a, (b, c))=((a, b), c)$

　　$aD(bDc)=(aDb)Dc$　　　　（结合律）

(c) $(ac, bc)=|c|(a, b)$

　　$(ca)D(cb)=|c|aDb$　　　　（分配律）

(d) $(a, 1)=(1, a)=1$ $(a, 0)=(0, a)=|a|$,

$aD1=1Da=1$, $aD0=0Da=|a|$.

证明 我们只证明(c)，其余几条的证明作为练习留给读者.

令$d=(a, b)$，$e=(ac, bc)$，我们需要证明$e=|c|d$.写$d=ax+by$. 我们有

(1) $cd=cax+cby$,

因为cd整除ac与bc二数，所以cd整除e. 又因为$e|ac$，$e|bc$，由(1)得$e|cd$，因此$|e|=|cd|$或者$e=|c|d$. □

定理1.5 Euclid引理. 如果$a|bc$且$(a, b)=1$，则有$a|c$.

证明 因为$(a, b)=1$，所以我们可以写$1=ax+by$，$c=acx+bcy$. 但$a|acx$，$a|bcy$，所以$a|c$. □

1.4 素数

定义 一个整数n被称为素数，若$n>1$且它的正约数只有1和n. 如果$n>1$且不是素数，则n称为复合数.

例如 100以内的素数有2，3，5，7，11，13，17，19，23，29，31，37，41，43，47，53，59，61，67，71，73，79，83，89，97.

注：通常用p，p'，p_i，q，q'，q_i表示素数.

定理1.6 任意一个整数$n>1$是素数或是一些素数的乘积，必是二者之一.

证明 我们对n作归纳法. 当$n=2$时，定理显然成立. 假定对$<n$的任意整数定理是成立的. 那么，当n不是素数

时，它有一个正约数$d\neq 1$，$d\neq n$，于是有$n=cd$，$n\neq c$．但c与d二数均$<n$且>1，所以c，d都是素数的乘积，因而n也是素数的乘积． □

定理1.7 Enclid定理．素数有无穷多个．

Euclid的证明 假设素数只有有限个，例如只有p_1，p_2，…，p_n，令$N=1+p_1p_2\cdots p_n$，于是$N>1$，所以N是素数或是一些素数之积．由于N大于每个素数p_i，N当然就不是素数，而且设有一个素数p_i整除N（如果$p_i|N$，那么p_i整除差$N-p_1p_2\cdots p_n=1$），与定理1.6矛盾． □

定理1.8 如果素数p不能整除a，那么$(p, a)=1$．

证明 令$d=(p, a)$，则$d|p$，所以$d=1$或$d=p$．但是$d|a$，所以$d\neq p$（因为$p\nmid a$），因此$d=1$． □

定理1.9 如果一个素数p整除ab，则有$p|a$或$p|b$．更一般，如果一个素数整除乘积$a_1a_2\cdots a_n$，则p至少整除其中一个因子．

证明 设$p|ab$且$p\nmid a$，我们证明$p|b$．由定理1.8，$(p, a)=1$，根据Euclid引理，得$p|b$．

对于更一般情形的证明，我们可以对因子的个数n作归纳法，详细证明留给读者。 □

1.5 算术基本定理

定理1.10 算术基本定理．每一个>1的整数n都能唯一地表示为素因数的乘积（不计因数的顺序）．

证明 我们对n作归纳法．当$n=2$时定理是成立的．假定对于大于1小于n的所以整数定理成立，我们要证明对于

n定理成立．如果n是素数就不必证了，于是假设n是复合数且n有两种分解式，

（2）$n=p_1p_2\cdots p_s=q_1q_2\cdots q_t$，

我们要证明$s=t$且每一个p等于某个q．因为p_1整除乘积$q_1q_2\cdots q_t$，所以p_1必整除其中至少一个因数，重排q_1，q_2，…，q_t的顺序，使$p_1|q_1$．因为p_1，q_1都是素数，所以$p_1=q_1$．（2）式两边消去p_1得

$$\frac{n}{p_1}=p_2\cdots p_s=q_2\cdots q_t.$$

若$S>1$或$t>1$，则$1<\frac{n}{p_1}<n$．归纳法假设告诉我们，除开因数的顺序外，$\frac{n}{P_1}$的两个分解式必须相同，因此$s=t$且不计因数的顺序，（2）的两个分解式是相同的．证明完成．

注：在整数n的分解式中，特定的素数p可以出现多次．如果n的不同的素因数是p_1，p_2，…，p_r，且p_i作为因数出现α_i次，则我们可以写

$$n=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_r^{\alpha_r},$$

或更简短地写为

$$n=\prod_{i=1}^{r}p_i^{\alpha_i}$$

这个式子叫做n的素数幂分解式．在这个式子中，我们取每个指数α_i为0也就可以表示1．

定理1.11　若$n=\prod_{i=1}^{r}p_i^{\alpha_i}$，则n的正约数的集合就是形如$\prod_{i=1}^{r}p_i^{c_i}$的数的集合，其中$0\leqslant c_i\leqslant\alpha_i$，$i=1$，2，…，r．

证明　留作练习．

注：如果我们把依次增大的素数系列记为

$p_1=2$，$p_2=3$，$p_3=5$，…，$p_n=$第n个素数，则每一个正整数n（包括1）

能表示为形式

$$n=\prod_{i=1}^{\infty}p_i^{\alpha_i},$$

其中每一个指数$\alpha_i\geqslant 0$，而n的正因数是形如

$$\prod_{i=1}^{\infty}p_i^{c_i}$$

的所有的数，证中$0\leqslant c_i\leqslant\alpha_i$，是个乘积自然是有限的．

定理1.12　如果两个正整数a与b的因子分解式为

$$a=\prod_{i=1}^{\infty}p_i^{a_i},\qquad b=\prod_{i=1}^{\infty}p_i^{b_i},$$

那么它们的最大公约数的因子分解式为

$$(a,\ b)=\prod_{i=1}^{\infty}p_i^{c_i},$$

其中每一个$c_i=\min\{a_i,\ b_i\}$即a_i与b_i中的较小者．

证明　令$d=\prod_{i=1}^{\infty}p_i^{c_i}$，因$c_i\leqslant a_i$，$c_i\leqslant b_i$，我们有$d|a$，$d|b$，所以d是a与b的一个公约数．又令e是a与b的任一公约数并记为$e=\prod_{i=1}^{\infty}p_i^{e_i}$，则$e_i\leqslant a_i$，$e_i\leqslant b_i$，所以$e_i\leqslant c_i$，于是$e|d$，所以d是a与b的最大公约数．

1.6　素数倒数的级数

定理1.13　无穷级数$\sum_{n=1}^{\infty}\frac{1}{p_n}$发散．

证明　关于这个定理的下面的简短证明是由Clarkson［11］作出的．我们假定这个级数收敛便得出矛盾．若级数收敛，则有一个整数K使得

$$\sum_{m=k+1}^{\infty}\frac{1}{p_m}<\frac{1}{2}.$$

令$Q=p_1\cdots p_k$并考虑数$1+nQ$，$n=1,2,\cdots$，这些数中没有一个都被p_1，p_2，$\cdots$，p_k中的任何一个整除，因此$1+nQ$的所有素因数出现在素数p_{k+1}，p_{k+2}，$\cdots$之中，所以对每一个$r\geqslant 1$，我们有

$$\sum_{n=1}^{r}\frac{1}{1+nQ}\leqslant\sum_{t=1}^{\infty}\left(\sum_{m=k+1}^{\infty}\frac{1}{p_m}\right)^t,$$

这是因为左边的和式的所有的项都包含在右边的和式的项中．但是，这个不等式的右端不超过收敛的几何级数

$$\sum_{t=1}^{\infty}\left(\frac{1}{2}\right)^t,$$

所以级数$\sum_{n=1}^{\infty}\frac{1}{HnQ}$的部分和有界并因此收敛．但这是一个矛盾，因为积分检验或极限比较检验证明了这个级数是发散的． □

注：这个级数的发散性是由Euler[20]在1737年首先证明的，它因显然得到存在无穷多个素数的Euclid定理而著名．

在下一章我们将得到一个渐近公式，它说明部分和$\sum_{k=1}^{n}\frac{1}{p_n}$与$\log(\log n)$一样趋于无穷．

1.7 Euclid算法

当a与b的素数幂分解式已给出时，定理1.12提供了计算最大公约数（a，b）的一个实际方法．但是所谈的计算需要得到素数幂分解式，而选择一种最少计算过程的方法是合符需要的．有一个有效的方法，即著名的Euclid算法，它不需要a与b的分解式．这个方法是在连续作除法的基础上并利

用下面的定理作成的.

定理1.14 除法算法. 给定整数a与b且$b>0$, 则存在唯一的一对整数q与r, 使得

$$a=bq+r \qquad 0\leqslant r<b,$$

而且, $r=0$当且仅当$b|a$.

注: 我们称q是以b去除a所得的商数, r是所得的余数.

证明 令S是由

$$S=\{y: y=a-bx, x\text{是整数}, y\geqslant 0\}$$

给出的非负整数的集合, 它是非空的, 所以它有一个最小元$a-bq$. 令$r=a-bq$, 则$a=bq+r$且$r\geqslant 0$. 现在我们证明$r<b$. 设$r\geqslant b$, 则$0\leqslant r-b<r$, 但$r-b\in S$, 这是因为$r-b=a-b(q+1)$. 因此$r-b$是S中比最小数r还要小的数, 这个矛盾证明了$r<b$. 这一对数q, r是唯一的. 如果有另一对数q', r', 那么$bq+r=bq'+r'$, 所以$b(q-q')=r'-r$, 于是$b|(r-r')$. 如果$r'-r\neq 0$, 则$b\leqslant|r-r'|$, 这是一个矛盾. 因此$r'=r$且$q'=q$. 最后, $r=0$当且仅当$b|a$是显然的事. □

注: 虽然定理1.14是一个存在性定理, 但它的证明实际上给出了计算商数q和余数r的一种方法. 我们由a减去b的足够多的倍数直到我们得到$a-bx$的最小的非负的数为止.

定理1.15 Euclid算法. 给定正整数a与b, 这里$b\nmid a$. 令$r_0=a$, $r_1=b$, 反复利用除法算法得到由关系式

$$\begin{array}{ll}
r_0=r_1q_1+r_2 & 0<r_2<r_1\\
r_1=r_2q_2+r_3 & 0<r_3<r_2\\
\cdots\cdots & \cdots\cdots\\
r_{n-2}=r_{n-1}q_{n-1}+r_n & 0<r_n<r_{n-1}\\
r_{n-1}=r_nq_n+r_{n+1} & r_{n+1}=0
\end{array}$$

逐次确定的余数r_2，r_3，…，r_n，r_{n+1}的集合．则最后的非零的余数r_n就是a与b的最大公约数（a，b）．

证明　因为r_i是递减非负的，所以必有一步得$r_{n+1}=0$．最后一个式子$r_{n-1}=r_nq_n$说明$r_n|r_{n-1}$，倒数第二个式子说明$r_n|r_{n-2}$．由归纳法我们看到r_n整除每一个r_i，特别地，$r_n|r_1=b$，$r_n|r_0=a$，所以r_n是a与b的一个公约数．现在令d是a与b的任一公约数，由第一个式子$r_0=r_1q+r_2$说明$d|r_2$，下一个式子说明$d|r_3$，由此递推，d整除每一个r_i，所以$d|r_n$，于是r_n就是所求的最大公约数．□

1.8　两个以上的数的最大公约数

三个整数a，b，c的最大公约数用（a，b，c）表示并由下式定义：

$$(a, b, c)=(a, (b, c)).$$

根据定理1.4(b)我们有$(a, (b, c))=((a, b), c)$，所以最大公约数依赖于a，b，c而与它们的书写顺序无关．

同样，n个整数a_1，…，a_n的最大公约数由式子

$$(a_1, a_2, \cdots, a_n)=(a_1, (a_2, \cdots, a_n))$$

归纳定义，且它与a_i出现的顺序无关．

如果$d=(a_1, \cdots, a_n)$，容易验证d整除每一个a_i且它们的任一个公约数都整除d，并且d是a_i的一个线性组合，即存在整数x_1，…，x_n使得

$$(a_1, \cdots, a_n)=a_1x_1+\cdots+a_nx_n.$$

如果d＝1，这些数就称为是互素的．例如2，3和10是互素的．

如果$(a_i, a_j)=1$，这里$i\neq j$，则数a_1，…，a_n称为是两两互素的．若a_1，…，a_n是两两互素的，则$(a_1, \cdots, a_n)=1$．但是由例子（2，3，10）可说明反之并不一定成立．

第一章习题

本章习题中的小写拉丁字母 a，b，c，…，x，y，z 表示整数．

证明 1 — 6 题

1． 如果$(a, b)=1$，且$c|a$，$d|b$，则$(c, d)=1$．

2． 如果$(a, b)=(a, c)=1$，则$(a, bc)=1$．

3． 若$(a, b)=1$，则对所有的$n\geqslant 1$，$k\geqslant 1$，有$(a^n, b^k)=1$．

4． 若$(a, b)=1$，则$(a+b, a-b)$必为1或2．

5． 若$(a, b)=1$，则$(a+b, a^2-ab+b^2)$必为1或3．

6． 若$(a, b)=1$且$d|(a+b)$，则$(a, d)=(b, d)=1$．

7． 当$(a, b)=1$时，有理数$\frac{a}{b}$称为既约分数．如果两个既约分数的和是整数，比如$\left(\frac{a}{b}\right)+\left(\frac{c}{d}\right)=n$，证明$|b|=|d|$．

8． 一个整数若不能被任何一个素数的平方整除，这个整数就称为无平方因子数．证明，对每一个$n\geqslant 1$，存在唯一确定的$a>0$，$b>0$，使得$n=a^2b$，这里b是无平方因子数．

9． 对下面的每一条叙述，或者给出证明，或者举出一个反例．

(a) 若$b^2|n$，$a^2|n$，$a^2\leqslant b^2$，则$a|b$.

(b) 若b^2是n的最大的平方约数，则由$a^2|n$可得出$a|b$.

10. 已知x与y，设$m=ax+by$，$n=cx+dy$，这里$ad-bc=\pm1$，证明$(m, n)=(x, y)$.

11. 证明，当$n>1$时，n^4+4是复合数.

在12、13、14题中，a，b，c，m，n表示正整数.

12. 对下面的每一条叙述，或者给出证明，或者举出一个反例.

(a) 若$a^n|b^n$，则$a|b$.

(b) 若$n^n|m^n$，则$n|m$.

(c) 若$a^n|2b^n$，$n>1$，则$a|b$.

13. (a) 若$(a, b)=1$且$\left(\frac{a}{b}\right)^m=n$，证明$b=1$.

(b) 如果n不是一个正整数的m次方幂，证明$n^{\frac{1}{m}}$是无理数.

14. 如果$(a, b)=1$，$ab=c^n$，证明$a=x^n$，$b=y^n$对某个x与y成立. [提示：讨论$d=(a, c)$].

15. 证明每一个$n\geqslant12$是两个复合数之和.

16. 证明，若2^n-1是素数，则n也是素数.

17. 证明，若2^n+1是素数，则n是2的方幂.

18. 如果$m\neq n$，试算出以a表示的最大公约数$(a^{2^m}+1, a^{2^n}+1)$. [提示：令$A_n=a^{2^n}+1$并证明如果$m>n$，则有$A_n|(A_m-2)$].

19. Fibonacci序列1，1，2，3，5，8，13，21，34，… 是由递推公式$a_{n+1}=a_n+a_{n-1}$确定的，其中$a_1=a_2=1$.

证明，对每一个n都有$(a_n, a_{n+1})=1$。

20. 令$d=(826, 1890)$。利用Enclid算法计算d，并把d表示为826与1890的一个线性组合.

21. 两个整数a与b的最小公倍数(lcm)记为$[a, b]$或aMb，并由下式确定，

$$[a, b]=\frac{|ab|}{(a,b)} \quad 当a\neq0, b\neq0时,$$

$$[a, b]=0 \qquad 当a=0或b=0时,$$

证明最小公倍数有下列性质：

(a) 如果 $a=\prod_{i=1}^{\infty} p_i^{a_i}$，$b=\prod_{i=1}^{\infty} p_i^{b_i}$，

则$[a, b]=\prod_{i=1}^{\infty} p_i^{c_i}$，其中$c_i=\max\{a_i, b_i\}$。

(b) $(aDb)Mc=(aMc)D(bMc)$.

(c) $(aMb)Dc=(aDc)M(bDc)$.

（D与M是相互分配的）.

22. 证明，$(a, b)=(a+b, [a, b])$.

23. 两个正整数的和是5264而它们的最小公倍数是200340，试确定这两个数.

24. 证明下面的最大公约数的乘法性质：

$$(ah, bk)=(a, b)(h, k)\left(\frac{a}{(a,b)}, \frac{k}{(h,k)}\right)\left(\frac{b}{(a,b)}, \frac{h}{(h,k)}\right).$$

特别，当$(a, b)=(h, k)=1$时，这证明了$(ah, bk)=(a, k)(b, h)$.

证明从25题至28题的每一题．其中所有的整数都是正的．

25. 如果$(a, b)=1$，则存在$x>0$与$y>0$，使得$ax-by=1$

26. 如果$(a, b)=1$，$x^a=y^b$，则对某个n有$x=n^b$，$y=n^a$. [利用25题与13题].

27. (a) 若$(a, b)=1$，则对每个$n>ab$，存在正整数x与y，使得$n=ax+by$.

    (b) 若$(a, b)=1$，则没有正整数x与y使得
    $ab=ax+by$.

28. 若$a>1$，则$(a^m-1, a^n-1)=a^{(m,n)}-1$.

29. 给定$n>0$，令S是元素$\leqslant 2n$的一个正整数集合，使得如果a，b属于S，$a\neq b$，则$a\nmid b$. 问S包含的整数最多有多少个？[提示：S最多只能包含$1, 2, 2^2, 2^3, \cdots$中的一个. 同样，最多只能包含$3, 3.2, 3.2^2, \cdots$中的一个，等等.]

30. 如$n>1$，证明和

$$\sum_{k=1}^{n}\frac{1}{k}$$

不是一个整数.

第二章　数论函数与Dirichlet乘积

2.1　引言

数论，与数学的其它许多分支一样，经常涉及到实数或复数序列．在数论中，这样的序列称为数论函数．

定义　在正整数上定义的实值的或复值的函数称为数论函数或算术函数．

本章介绍几个数论函数，它们在整数的整除性以及素数分布的讨论中起重要作用．本章也讨论Dirichlet乘积，这个概念将帮助我们阐明不同的数论函数之间的相互关系的性质．

我们首先从两个重要的例子开始，这就是Möbius函数$\mu(n)$与Euler函数$\varphi(n)$．

2.2　Möbius函数$\mu(n)$

定义　Möbius函数μ的定义如下：

$\mu(1)=1$；

如果$n>1$，写$n=p_1^{\alpha_1}\cdots p_k^{\alpha_k}$，则

$\mu(n)=(-1)^k$　当$\alpha_1=\alpha_2=\cdots=\alpha_k=1$时，

$\mu(n)=0$　　　　其它.

注意　$\mu(n)=0$当且仅当n有一个>1的平方因子.

下面是$\mu(n)$的值的一个短表:

n:	1	2	3	4	5	6	7	8	9	10
$\mu(n)$:	1	−1	−1	0	−1	1	−1	0	0	1

Möbius 函数在数论中经常出现，它的基本性质之一是对约数求和$\sum_{d\mid n}\mu(d)$的一个重要的简明的公式，它在n的正约数上展开，式中的[x]表示$\leqslant x$的最大整数.

定理2.1　如果$n\geqslant 1$，我们有

$$\sum_{d\mid n}\mu(d)=\left[\frac{1}{n}\right]=\begin{cases}1 & 当n=1时\\ 0 & 当n>1时.\end{cases}$$

证明　对于$n=1$，等式显然成立. 设$n>1$并写$n=p_1^{\alpha_1}\cdots p_k^{\alpha_k}$，在和$\sum_{d\mid n}\mu(d)$中非零的项仅来自$d=1$与n的约数是不同素数的乘积，即

$$\begin{aligned}\sum_{d\mid n}\mu(d)&=\mu(1)+\mu(p_1)+\cdots+\mu(p_k)+\mu(p_1p_2)+\\&\quad\cdots+\mu(p_{k-1}p_k)+\cdots+\mu(p_1p_2\cdots p_k)\\&=1+\binom{k}{1}(-1)+\binom{k}{2}(-1)^2+\cdots\\&\quad+\binom{k}{k}(-1)^k=(1-1)^k\\&=0\end{aligned}$$

□

2.3　Euler函数φ(n)

定义　$n>1$，Euler函数$\varphi(n)$定义为不大于n并与n互

素的数的个数，即

(1) $\varphi(n)=\sum_{k=1}^{n}{}'1$,

其中，表示和式在与n互素的那些K上展开．下面是$\varphi(n)$的值的一个短表：

n:	1	2	3	4	5	6	7	8	9	10
$\varphi(n)$:	1	1	2	2	4	2	6	4	6	4

与$\mu(n)$相似，有一个对约数求和$\sum_{d\mid n}\varphi(d)$的一个简单公式．

定理2.2　如果$n\geqslant 1$，我们有

$$\sum_{d\mid n}\varphi(d)=n.$$

证明　令S表示集合$\{1, 2, \cdots, n\}$，我们把S中的整数分为下面一些互不相交的集合．对于n的每一个约数d，令

$$A(d)=\{k:(k, n)=d, 1\leqslant k\leqslant n\},$$

于是，$A(d)$包含了S中与n的最大公约数为d的那些元素，这些集合$A(d)$互不相交且它们的并集是S．因此，如果$f(d)$表示$A(d)$中整数的个数，我们就有

(2) $\sum_{d\mid n}f(d)=n$.

但$(k, n)=d$当且仅当$\left(\frac{k}{d}, \frac{n}{d}\right)=1$，而$0<k\leqslant n$当且仅当$0<\frac{k}{d}\leqslant\frac{n}{d}$．因此，如果我们令$q=\frac{k}{d}$，则在$A(d)$的元素与满足$0<q\leqslant\frac{n}{d}$，$\left(q, \frac{n}{d}\right)=1$的整数q之间有一个一一对应关系．这样的q的个数就是$\varphi\left(\frac{n}{d}\right)$，于是$f(d)=$

$\varphi\left(\frac{n}{d}\right)$且(2)变为

$$\sum_{d\mid n}\varphi\left(\frac{n}{d}\right)=n.$$

这与式子$\sum\limits_{d\mid n}\varphi(d)=n$相同，因为当d取遍n的所有约数时，$\frac{n}{d}$也取遍n的所有约数．证明完成． □

2.4 φ与μ的相互关系

Euler函数与Möbius函数通过下面公式相联系：

定理2.3 如果$n\geqslant 1$，则有

$$\varphi(n)=\sum_{d\mid n}\mu(d)\frac{n}{d}.$$

证明 和式(1)定义的$\varphi(n)$能改写为

$$\varphi(n)=\sum_{k=1}^{n}\left[\frac{1}{(n,k)}\right],$$

其中k通过所有$\leqslant n$的正整数．现在我们利用定理2.1并用(n,k)代替其中的n，得

$$\varphi(n)=\sum_{k=1}^{n}\sum_{d\mid(n,k)}\mu(d)=\sum_{k=1}^{n}\sum_{\substack{d\mid n\\ d\mid k}}\mu(d).$$

对于n的一个固定的约数d，我们必须对满足$1\leqslant k\leqslant n$并是d的倍数的k求和．如果我们写$k=qd$，则$1\leqslant k\leqslant n$当且仅当$1\leqslant q\leqslant\frac{n}{d}$，因此，$\varphi(n)$的和式最后可写为

$$\varphi(n)=\sum_{d\mid n}\sum_{q=1}^{n/d}\mu(d)=\sum_{d\mid n}\mu(d)\sum_{q=1}^{n/d}1$$

$$=\sum_{d\mid n}\mu(d)\frac{n}{d}.$$

定理得证．

2.5 φ(n)的一个乘积公式

定理2.3里φ(n)的和式也可表为在n的不同素约数上展开的乘积.

定理2.4 对n>1，我们有

(3) $\varphi(n)=n\prod_{p\mid n}\left(1-\frac{1}{p}\right)$.

证明，对n=1，因为没有素数整除1，故乘积无意义，在此情况下，指定乘积的值为1，这是可以理解的.

于是假设n>1并令p_1，…，p_r是n的不同素约数，乘积能写为

(4) $$\prod_{p\mid n}\left(1-\frac{1}{p}\right)=\prod_{i=1}^{r}\left(1-\frac{1}{p_i}\right)$$

$$=1-\sum\frac{1}{p_i}+\sum\frac{1}{p_ip_j}$$

$$-\sum\frac{1}{p_ip_jp_k}+\cdots+\frac{(-1)^r}{p_1p_2\cdots p_k},$$

在右端，比如$\sum\frac{1}{p_ip_jp_k}$这样一项里，它表示每次取n的三个不同素约数的乘积$p_ip_jp_k$. 注意(4)式右端每一项都是$\pm\frac{1}{d}$的形式，其中d是n的约数，它为1或不同素数的乘积，分子±1恰好是μ(d)，因为，如果d能被任一p_i的平方整除，则μ(d)=0. 这样，(4)式中的和恰好与

$$\sum_{d\mid n}\frac{\mu(d)}{d}$$

相同. 定理得证. □

$\varphi(n)$的许多性质可由这个乘积公式顺利推导出来．其中一些列入下面的定理．

定理2.5　Euler函数具有下列性质：

(a) 对于素数P与$\alpha \geqslant 1$，有$\varphi(P^{\alpha}) = P^{\alpha} - P^{\alpha-1}$．

(b) $\varphi(mn) = \varphi(m)\varphi(n)\left(\dfrac{d}{\varphi(d)}\right)$，这里$d=(m,n)$．

(c) $\varphi(mn) = \varphi(m)\varphi(n)$，如果$(m, n)=1$．

(d) $a|b$得出$\varphi(a)|\varphi(b)$．

(e) 当$n \geqslant 3$时，$\varphi(n)$是偶数．而且，如果n有r个不同的奇素因子时，$\alpha^{r}|\varphi(n)$．

证明　在(3)式里取$n=P^{\alpha}$即得(a)．为了证明(b)，我们写

$$\frac{\varphi(n)}{n} = \prod_{p|n}\left(1-\frac{1}{P}\right).$$

其次我们注意到，mn的每一个素因数也是m或n的素因数，而整除m与n二数的素数也整除(m, n)，因此，

$$\frac{\varphi(mn)}{mn} = \prod_{p|mn}\left(1-\frac{1}{P}\right)$$

$$= \frac{\prod_{p|m}\left(1-\frac{1}{P}\right)\prod_{p|n}\left(1-\frac{1}{P}\right)}{\prod_{p|mn}\left(1-\frac{1}{P}\right)}$$

$$= \frac{\dfrac{\varphi(m)}{m}\cdot\dfrac{\varphi(n)}{n}}{\dfrac{\varphi(d)}{d}}$$

于是我们得到(b)．而(c)是(b)的特殊情形．

下面我们由(b)去推出(d)．因为$a|b$，我们有$b=ac$，

这里$1\leqslant c\leqslant b$. 如果$c=b$，则$a=1$因而(d)成立. 如果$c<b$，由(b)有

$$(5)\quad \varphi(b)=\varphi(ac)=\varphi(a)\varphi(c)\frac{d}{\varphi(d)}$$
$$=d\varphi(a)\frac{\varphi(c)}{\varphi(d)},$$

其中$d=(a, c)$. 于是可对b作归纳法得到结果. 对$b=1$，则$a=1$，所以(d)成立. 假设对所有小于b的整数，(d)式成立，那么它对于c是成立，所以$\varphi(d)|\varphi(c)$，这因为$d|c$. 因此(5)式右边的数是$\varphi(a)$的倍数，即$\varphi(a)|\varphi(b)$. 这证明了(d).

现在我们证明(e). 若$n=2^\alpha$，$\alpha\geqslant 2$. 由(a)和$\varphi(n)$是偶数. 若n至少有一个奇素数因子，我们写

$$\varphi(n)=n\prod_{p|n}\frac{p-1}{p}=\frac{n}{\prod\limits_{p|n}p}\prod_{p|n}(p-1)$$
$$=C(n)\prod_{p|n}(p-1)$$

其中$C(n)$是一个整数，与$C(n)$相乘的数是偶数，所以$\varphi(n)$是偶数. 此外，对每一个奇素因子P，这个乘积给出一个因子2. 如果n有r个不同的奇素数因子，就有$2^r|\varphi(n)$. □

2.6 数论函数的Dirichlet乘积

在定理2.3中我们证明了

$$\varphi(n)=\sum_{d|n}\mu(d)\frac{n}{d},$$

右边的和式是数论中经常出现的一个类型，这些和有形式

$$\sum_{d\mid n} f(d)g\left(\frac{n}{d}\right),$$

其中f与g是数论函数，它们对于研究这些和的某些共同的性质是有价值的．今后我们将发现在 Dirichlet级数定理中很自然地会出现这一类型的和式．数论函数的乘积的一个新的性质对于处理这些和式是颇有用处的．它是由E.T.Bell[4]在1915年提出的一个观点．

定义 如果f与g是两个数论函数，我们规定它们的Dirichlet乘积（或译作卷积）是由等式

$$h(n)=\sum_{d\mid n} f(d)g\left(\frac{n}{d}\right)$$

确定的数论函数h(n)．

注：我们用$f*g$表示h并用$(f*g)(n)$代表h(n)，记号N表示数论函数$N(n)=n$，对所有的n.用这个记号，定理2.3可表示为

$$\varphi=\mu*N.$$

下面的定描述了Dirichlet乘积的代数性质．

定理2.6 Dirichlet乘积是可交换的与可结合的．即对任意的数论函数f，g，k，我们有

$$f*g=g*f \qquad \text{（交换律）},$$

$$(f*g)*k=f*(g*k) \qquad \text{（结合律）}.$$

证明 首先，我们注意到，$f*g$也可表示为

$$(f*g)(n)=\sum_{a\cdot b=n} f(a)g(b)$$

其中a与b通过所有的其乘积为n的正整数，这使交换律是不证自明的．

为了证明结合律，我们令$A=g*k$并讨论$f*A=f*(g*k)$，我们有

$$(f*A)(n)=\sum_{da=n} f(a)A(d)=\sum_{ad=n} f(a)\sum_{bc=d} g(b)k(c)$$
$$=\sum_{abc=n} f(a)g(b)k(c)$$

同样，我们令$B=f*g$并讨论$B*k$，对$(B*k)(n)$我们可导出与上式相同的式子，因此$f*A=B*k$，这说明Dirichlet乘积是可结合的. □

现在我们介绍这个乘法的一个单位元.

定义 由

$$I(n)=\left[\frac{1}{n}\right]=\begin{cases}1 & n=1\\ 0 & n>1\end{cases}$$

给定的数论函数I称为恒等函数.

定理2.7 对所有的，我们有$I*f=f*I=f$.

证明 我们有

$$(f*I)(n)=\sum_{d\mid n} f(d)I\left(\frac{n}{d}\right)=\sum_{d\mid n} f(d)\left[\frac{d}{n}\right]=f(n),$$

这因为，当$d<n$时，$\left[\frac{d}{n}\right]=0$. □

2.7 Dirichlet逆函数与Möbius反转公式

定理2.8 如果f是一个数论函数且$f(1)\neq 0$，则存在唯一的一个被称为f的Dirichlet逆函数的数论函数，使得

$$f*f^{-1}=f^{-1}*f=I,$$

还有，f^{-1}由递推公式

$$f^{-1}(1)=\frac{1}{f(1)},\quad f^{-1}(n)=\sum_{\substack{d\mid n\\ d<n}} f\left(\frac{n}{d}\right)f^{-1}(d)$$

对$n>1$

给出.

证明　给定f，我们将证明方程$(f*f^{-1})(n)=I(n)$对函数值$f^{-1}(n)$有唯一解．对$n=1$，方程$(f*f^{-1})(1)=I(1)$化为$f(1)f^{-1}(1)=1$．因为$f(1)\neq 0$，所以有且仅有一个解$f^{-1}(1)=\frac{1}{f(1)}$．现在假设对所有的$k<n$，函数值$f^{-1}(k)$是唯一确定的，那么我们必须解方程$(f*f^{-1})(n)=I(n)$或

$$\sum_{d\mid n} f\left(\frac{n}{d}\right)f^{-1}(d)=0,$$

这个方程可写为

$$f(1)f^{-1}(n)+\sum_{\substack{d\mid n\\ d<n}} f\left(\frac{n}{d}\right)f^{-1}(d)=0.$$

如果对所有的约数$d<n$，函数值$f^{-1}(d)$是已知的，那么，存在唯一确定的函数值$f^{-1}(n)$，即

$$f^{-1}(n)=\frac{-1}{f(1)}\sum_{\substack{d\mid n\\ d<n}} f\left(\frac{n}{d}\right)f^{-1}(d),$$

这因为$f(1)\neq 0$．由归纳法，f^{-1}的存在性与唯一性是成立的．

注：我们有$(f*g)(1)=f(1)\neq g(1)$，因此，如果$f(1)\neq 0$且$g(1)0$，则$(f*g)(1)\neq 0$.这个事实与定理2.6，2.7，2.8告诉我们，用群论的语言来讲，所有数论函数$f(f(1)\neq 0)$的集合关于运算*形成一个Abel群，其恒等元为I.读者容易验证，

$$(f*g)^{-1}=f^{-1}*g^{-1}\qquad 当f(1)\neq 0,g(1)\neq 0时.$$

定义　我们规定单位函数u是对所有的n都有$u(n)=1$的数论函数.

定理2.1说明$\sum_{d\mid n}\mu(d)=I(n)$，用Dirichlet记号，此式就写为$\mu*u=I$，于是u与$\mu$互为Dirichlet逆函数：

$$u=\mu^{-1}\qquad 与\qquad \mu=u^{-1}.$$

Möbius函数的这个简单性质与Dirichlet乘积的 结合律使我们能给出下面定理的一个简单的证明.

定理2.9 Möbius反转公式. 由等式

(6) $f(n)=\sum_{d\mid n}g(d)$

可推出

(7) $g(n)=\sum_{d\mid n}f(d)\mu\left(\frac{n}{d}\right)$,

反之, 由(7)可推出(6).

证明 等式(6)即$f=g*u$, 用μ去乘, 得$f*\mu=(g*u)\mu=g*(u*\mu)=g*I=g$, 这就是(7)式. 反之, 用$u$去乘$f*\mu=g$就得到(6)式.

Möbius反转公式可以用前面的定理2.2与2.3的两个公式来说明:

$$n=\sum_{d\mid n}\varphi(d),\qquad \varphi(n)=\sum_{d\mid n}d\mu\left(\frac{n}{d}\right).$$

2.8 Mangoldt函数$\Lambda(n)$

下面我们介绍Mangoldt函数Λ,它在素数分布的理论中起着重要作用.

定义 对每一个整数$n>1$, 我们定义

$$\Lambda(n)=\begin{cases}\log p & n=p^m,\ p\text{为素数},\ m\geqslant 1\\ 0 & \text{其它}.\end{cases}$$

下面是$\Lambda(n)$的值的一个短表

n:	1	2	3	4	5	6	7	8	9	10
$\Lambda(n)$:	0	lg2	lg3	lg2	lg5	0	lg7	lg2	lg3	0

下面定理的证明说明这个函数自然是由算术基本定理产生

的.

定理2.10　若n≥1，则我们有

(8) $\log n=\sum_{d\mid n}\Lambda(d)$.

证明　如果n＝1，因为两边都是0，所以等式成立.

假设n＞1并写$n=\prod_{k=1}^{r}p_k^{\alpha_k}$,

取对数，我们有

$$\log n=\sum_{k=1}^{r}\alpha_k\log p_k.$$

现在讨论(8)式右端的和，其中仅有的非零的项来自形如$p_k^m(m=1,2,\cdots,\alpha_k,k=1,2,\cdots,r)$的这些约数d．因此,

$$\sum_{d\mid n}\Lambda(d)=\sum_{k=1}^{r}\sum_{m=1}^{\alpha_k}\Lambda(p_k^m)=\sum_{k=1}^{r}\sum_{m=1}^{\alpha_k}\log p_k$$

$$=\sum_{k=1}^{r}\alpha_k\log p_k=\log n.$$

这证明(8)成立.

现在我们利用μöbius反转公式并用对数来表示Λ(n).

定理2.11　如果n≥1，我们有

$$\Lambda(n)=\sum_{d\mid n}\mu(d)\log\frac{n}{d}=-\sum_{d\mid n}\mu(d)\log d.$$

证明　对(8)式用μöbius反转公式，我们得到

$$\Lambda(n)=\sum_{d\mid n}\mu(d)\mathrm{lod}\frac{n}{d}$$

$$=\log n\sum_{d\mid n}\mu(d)-\sum_{d\mid n}\mu(d)\log d$$

$$=I(n)\log n-\sum_{d\mid n}\mu(d)\log d.$$

因为对所有的n，I(n)logn＝0，所以证明完成.

2.9 积性函数

我们已经注意到，具有$f(1)\neq 0$的所有数论函数f的集合对于Dirichlet乘法形成一个Abel群. 本节讨论这个群的一个重要的称为积性函数的子群.

定义 一个数论函数f被称为是积性的，如果f不恒为零并且对任意的$(m,n)=1$，有$f(mn)=f(m)f(n)$.

一个积性函数被称为是完全积性的，如果对所有的m，n，都有$f(mn)=f(m)f(n)$.

例 1 令$f_\alpha(n)=n^\alpha$，这里α是一个固定的实数或复数. 这个函数是完全积性的. 特别，单位函数$u=f_0$是完全积性的. 我们用N^α表示函数f_α并称它为幂函数.

例 2 恒等函数$I(n)=\left[\frac{1}{n}\right]$是完全积性的.

例 3 Möbius函数是积性的但不是完全积性的. 这由$\mu(n)$的定义容易看出. 考虑两个互素的整数m与n. 若m或n中任何一个有约数为一个素数的平方，则mn也有，并且$\mu(mn)$与$\mu(m)\mu(n)$都为零. 若二者都没有素数平方因数，记$m=p_1\cdots p_s$，$n=q_1\cdots q_t$，这里p_i与q_i是不同的素数，则$\mu(m)=(-1)^s$，$\mu(n)=(-1)^t$且$\mu(mn)=(-1)^{s+t}=\mu(m)\mu(n)$，这证明了$\mu$是积性函数. 又因为$\mu(4)=0$，而$\mu(2)\mu(2)=1$，所以它不是完全积性的.

例 4 Euler函数$\varphi(n)$是积性的，这是定理2.5的(c). 又因$\varphi(4)=2$而$\varphi(2)\varphi(2)=1$，故它不是完全积性的.

例 5 两个数论函数f与g的普通乘积是用通常的公式定义的：

$$(fg)(n)=f(n)g(n).$$

类似地，商$\frac{f}{g}$是由公式

$$\left(\frac{f}{g}\right)(n)=\frac{f(n)}{g(n)} \qquad g(n)\neq 0$$

定义的．如果f与g是积性的，则fg与$\frac{f}{g}$也是积性的．如果f与g是完全积性的，则fg与$\frac{f}{g}$也是完全积性的．

现在我们推导出积性函数的一些共同性质．

定理2.12 若f是积性函数，则$f(1)=1$.

证明 对所有的n，因为$(n,1)=1$，我们有$f(n)=f(1)f(n)$．由于f是不恒等于零的，所以有某个n，使$f(n)\neq 0$，于是$f(1)=1$. □

注：因为$\Lambda(1)=0$，故Mangoldt函数不是积性的．

定理2.13 给定f且$f(1)=1$，则

(a) **f是积性的当且仅当**

$$f(p_1^{\alpha_1}\cdots p_r^{\alpha_r})=f(p_1^{\alpha_1})\cdots f(p_r^{\alpha_r})$$

对所有的素数p_i与所有的整数$\alpha_i\geq 1$成立．

(b) **如果f是积性的，则f是完全积性的当且仅当**

$$f(p^\alpha)=f(p)^\alpha$$

对所有的素数p与所有的整数$\alpha\geq 1$成立．

证明 此证明由定义易于得出并留给读者作为练习．

2.10 积性函数与Dirichlet乘积

定理2.14 如果f与g是积性的，那么它们的Dirichlet

乘积也是积性的

证明　令$h=f*g$且选取互素的整数m与n，则

$$h(mn)=\sum_{c\mid mn}f(c)g\left(\frac{mn}{c}\right).$$

于是mn的每一个约数c能写为$c=ab$，这里$\frac{a}{m}$　$b|n$，$(a,b)=1$，$\left(\frac{m}{a},\ \frac{n}{b}\right)=1$并且在乘积$ab$的集合与$mn$的约数$c$之间有一一对应，因此

$$\begin{aligned}h(mn)&=\sum_{\substack{a\mid m\\ b\mid n}}f(ab)g\left(\frac{mn}{ab}\right)\\&=\sum_{\substack{a\mid m\\ b\mid n}}f(a)f(b)g\left(\frac{m}{a}\right)g\left(\frac{n}{b}\right)\\&=\sum_{a\mid n}f(a)g\left(\frac{m}{a}\right)\sum_{b\mid n}f(b)g\left(\frac{n}{b}\right)\\&=h(m)h(n)\end{aligned}$$

证明完成．　□

注意，两个完全积性函数的Dirichlet乘积不一定是完全积性的．

上面的证明作些微小的修改便能证明下面的

定理2.15　如果g与$f*g$都是积性的，则f也是积性的．

证明　我们假设f不是积性的并推出$f*g$也不是积性的．令$h=f*g$，因为f不是积性的，故存在正整数$m,n,(m,n)=1$，使得

$$f(mn)\neq f(m)f(n).$$

我们选取这样一对m,n,使其乘积mn尽可能地小．如果$mn=1$，则$f(1)\neq f(1)f(1)$，所以，$f(1)\neq 1$．因为$h(1)=f(1)g(1)=f(1)\neq 1$，所以h不是积性的．

如果$mn>1$，则对所有的满足条件$(a,b)=1$，$ab<mn$的正整数a与b，有$f(ab)=f(a)f(b)$，同定理2.14的证明一样，我们把确定$h(mn)$的和中对应于$a=m$，$b=n$的一项分离出去，我们有

$$
\begin{aligned}
h(mn) &= \sum_{\substack{a \mid m \\ b \mid n \\ ab<mn}} f(ab)g\left(\frac{mn}{ab}\right)+f(mn)g(1) \\
&= \sum_{\substack{a \mid m \\ b \mid n \\ ab<mn}} f(a)f(b)g\left(\frac{m}{a}\right)g\left(\frac{n}{b}\right)+f(mn) \\
&= \sum_{a \mid m} f(a)g\left(\frac{m}{a}\right)\sum_{b \mid n} f(b)g\left(\frac{n}{b}\right) \\
&\quad -f(m)f(n)+f(mn) \\
&= h(m)h(n)-f(m)f(n)+f(mn).
\end{aligned}
$$

因为$f(mn)\neq f(m)f(n)$，所以$h(mn)\neq h(m)h(n)$．所以h不是积性的．这个矛盾使证明完成． □

定理2.6　如果g是积性的，那么它的Dirichlet逆函数g^{-1}也是积性的．

证明　因为g与$g*g^{-1}=I$都是积性的，由定理2.15就得到这个证明． □

注：定理2.14与定理2.16说明积性函数的集合是$f(1)\neq 0$的所有的数论函数f作成的群的一个子群．

2.11　完全积性函数的逆函数

完全积性函数的Dirichlet逆函数特别容易确定．

定理2.17　令f是积性的，则f是完全积性的当且仅当

$$f^{-1}(n)=\mu(n)f(n)\qquad \text{对所有的}n\geq 1.$$

证明　令$g(n)=\mu(n)f(n)$. 如果f是完全积性的，则有

$$(g*f)(n)=\sum_{d\mid n}\mu(d)f(d)f\left(\frac{n}{d}\right)=f(n)\sum\mu(d)$$
$$=f(n)I(n)=I(n),$$

这因为$f(1)=1$而对$n>1$有$f(n)=0$. 于是$g=f^{-1}$.

反之，设$f^{-1}(n)=\mu(n)f(n)$，为说明f是完全积性的，只须证明对所有的素数的方幂有$f(p^{\alpha})=f(p)^{\alpha}$就够了. 等式$f^{-1}(n)=\mu(n)f(n)$即

$$\sum_{d\mid n}\mu(d)f(d)f\left(\frac{n}{d}\right)=0\quad 对所有的n>1.$$

于是取$n=p^{\alpha}$，我们有

$$\mu(1)f(1)f(p^{\alpha})+\mu(p)f(p)f(p^{\alpha-1})=0.$$

由此得　$f(p^{\alpha})=f(p)f(p^{\alpha-1})$，即$f(p^{\alpha})=f(p)^{\alpha}$，所以f是完全积性的. □

例　Euler函数φ的逆函数. 因为$\varphi=\mu*N$,所以有$\varphi^{-1}=\mu^{-1}*N^{-1}$. 但因N是完全积性的，$N^{-1}=\mu N$，所以

$$\varphi^{-1}=\mu^{-1}*\mu N=u*\mu N,$$

因此

$$\varphi^{-1}(n)=\sum_{d\mid n}d\mu(d).$$

下一个定理指出

$$\varphi^{-1}(n)=\prod_{p\mid n}(1-p).$$

定理2.18　如果f是积性的，则有

$$\sum_{d\mid n}\mu(d)f(d)=\prod_{p\mid n}(1-f(p)).$$

证明　令

$$g(n)=\sum_{d\mid n}\mu(d)f(d).$$

则g是积性的，所以，为确定g(n)只需计算$g(p^\alpha)$就够了.但是

$$g(p^\alpha)=\sum_{d\mid p^\alpha}\mu(d)f(d)=\mu(1)f(1)+\mu(p)f(p)$$
$$=1-f(p).$$

于是

$$g(n)=\prod_{p\mid n}g(p^\alpha)=\prod_{p\mid n}(1-f(p)).\qquad\square$$

2.12 Liouville函数λ(n)

完全积性函数的一个重要例子是Liouville函数λ，其定义如下：

定义 我们规定λ(1)=1，如果$n=p_1^{\alpha_1}\cdots p_k^{\alpha_k}$，我们规定

$$\lambda(n)=(-1)^{\alpha_1+\cdots+\alpha_k}.$$

此定义即可说明λ是完全积性的，下一个定理刻划了约数的λ之和.

定理2.19 对每一个n>1，我们有

$$\sum_{d\mid n}\lambda(d)=\begin{cases}1 & \text{n是平方数,}\\ 0 & \text{其它.}\end{cases}$$

还有，$\lambda^{-1}(n)=|\mu(n)|$**对所有的n.**

证明：令$g(n)=\sum_{d\mid n}\lambda(d)$，则g是积性的.所以，为确定g(n)，我们只需计算素数幂的$g(p^\alpha)$，我们有

$$g(p^\alpha)=\sum_{d\mid p^\alpha}\lambda(d)=1+\lambda(p)+\lambda(p^2)+\cdots+\lambda(p^\alpha)$$
$$=1-1+1-\cdots(-1)^\alpha=\begin{cases}0 & \alpha\text{是奇数,}\\ 1 & \alpha\text{是偶数.}\end{cases}$$

因此，如果$n=\prod_{i=1}^{k}p_i^{\alpha_i}$，我们有$g(n)=\prod_{i=1}^{k}g(p_i^{\alpha_i})$.
如果有某个指数α_α是奇数，则$g(p_i^{\alpha_i})=0$，因而，$g(n)=0$。
如果所有的α_i都是偶数，则对所有的i，都有$g(p_i^{\alpha_i})=1$，所以$g(n)=1$，这说明，如果n是平方数，则$g(n)=1$，其余的$g(n)=0$. 而且$\lambda^{-1}(n)=\mu(n)\lambda(n)=\mu^2(n)=|\mu(n)|$.

2.13 除数函数$\sigma_\alpha(n)$

定义 对于实数或复数α以及任意整数$n\geq 1$，我们规定

$$\sigma_\alpha(n)=\sum_{d\mid n}d^\alpha$$

为n的约数的α次方幂的和.

这样定义的函数σ_α称为除数函数，它们都是积性的，因为$\sigma_\alpha=u*N^\alpha$是两个积性函数的Dirichlet乘积.

当$\alpha=0$时，$\sigma_0(n)$是n的约数的个数，常用$d(n)$表示。

当$\alpha=1$时，$\sigma_1(n)$是n的约数之和，常用$\sigma(n)$表示.

因为σ_α是积性的，我们有

$$\sigma_\alpha(p_1^{a_1}\cdots p_k^{a_k})=\sigma_\alpha(p_1^{a_1})\cdots\sigma_\alpha(p_k^{a_k}).$$

为计算$\sigma_\alpha(p^a)$，我们注意到p^a的约数是

$$1,\ p,\ p^2,\ \cdots,\ p^a,$$

因此，

$$\sigma_\alpha(p^a)=1^\alpha+p^\alpha+p^{2\alpha}+\cdots+p^{a\alpha}$$

$$=\frac{p^{\alpha(a+1)}-1}{p^\alpha-1}\qquad 如果\alpha\neq 0$$

$$=a+1\qquad 如果\alpha=0.$$

σ_α的Dirichlet逆函数也可表为n的约数的α次方幂的线性组合.

定理2.20　对$n\geq1$，我们有

$$\sigma_\alpha^{-1}(n)=\sum_{d|n}d^\alpha\mu(d)\mu\left(\frac{n}{d}\right).$$

证明　因为$\sigma_\alpha=N^\alpha*u$并且N^α是完全积性的，所以我们有

$$\sigma_\alpha^{-1}=(\mu N^\alpha)*u^{-1}=(\mu N^\alpha)*\mu. \qquad \square$$

2.14 广义卷积

本节内，F表示一个定义在正实轴$(0,+\infty)$上的实的或复值函数，使得对$0<x<1$，有$F(x)=0$.这种类型的和

$$\sum_{n\leq x}\alpha(n)F\left(\frac{x}{n}\right)$$

在数论中经常出现，其中α是任意的数论函数.这样的和在$(0,+\infty)$上确定一个新函数G，且对于$0<x<1$，$G(x)$也为零.我们用$\alpha o F$表示这个函数G.这样，

$$\alpha oF(x)=\sum_{n\leq x}\alpha(n)F\left(\frac{x}{n}\right).$$

如果对所有的非整数x，$F(x)=0$，则F限制在整数上是一个数论函数，并有

$$(\alpha oF)(m)=(\alpha*F)(m)$$

对所有的整数$m\geq1$成立.所以运算o能被看作是Dirichlet乘积*的推广.

一般说来，运算o是可交换而不可结合的.但是，下面

的定理可作为结合律的替换形式。

定理2.21　关于o与*的结合性．对任意数论函数α与β，我们有

(9)　$\alpha o(\beta o F)=(\alpha*\beta)oF.$

证明　对x>0，我们有

$$\left\{\alpha o(\beta o F)\right\}(x)=\sum_{n\le x}\alpha(n)\sum_{m\le\frac{x}{n}}\beta(m)F\left(\frac{x}{mn}\right)$$

$$=\sum_{mn\le x}\alpha(n)\beta(m)F\left(\frac{x}{mn}\right)$$

$$=\sum_{k\le x}\left(\sum\alpha(n)\beta\left(\frac{k}{n}\right)\right)F\left(\frac{x}{k}\right)$$

$$=\sum_{k\le x}(\alpha*\beta)(k)F\left(\frac{x}{k}\right)$$

$$=\{(\alpha*\beta)oF\}(x).$$

证明完成．　□

下面我们注意到，Dirichlet乘积的恒等函数 $I(n)=\left[\frac{1}{n}\right]$对运算．也是恒等的，即有

$$(IoF)(x)=\sum_{n\le x}\left[\frac{1}{n}\right]F\left(\frac{x}{n}\right)=F(x).$$

现在，我们利用这个事实连同结合性一起去证明下面的反转公式．

定理2.22　广义反转公式．如果α有一个Dirichlet逆函数α^{-1}，则等式

(10)　$G(x)=\sum_{n\le x}\alpha(n)F\left(\frac{x}{n}\right)$

可推出

$$(11)\quad F(x)=\sum_{n\leq x}\alpha^{-1}(n)G\left(\frac{x}{n}\right).$$

反之，由(11)可推出(10).

证明　如果$G=\alpha\text{o}F$，则

$$\alpha^{-1}\text{o}G=\alpha^{-1}\text{o}(\alpha\text{o}F)=(\alpha^{-1}*\alpha)\text{o}F=I\text{o}F=F.$$

这就由(10)推出(11). 反之，可类似地证明. □

下面的特殊情形尤为重要.

定理2.23　广义的Möbius反转公式，如果α是完全积性的，则有

$$G(x)=\sum_{n\leq x}\alpha(n)F\left(\frac{x}{n}\right)\text{当且仅当}F(x)$$

$$=\sum_{n\leq x}\mu(n)\alpha(n)G\left(\frac{x}{n}\right).$$

证明　在此情况下，$\alpha^{-1}(n)=\mu(u)\alpha(n)$. □

2.15　形式幂级数

在微积分里，形如

$$(12)\quad \sum_{n=0}a_nx^n=a(0)+a(1)x+a(2)x^2+\cdots+a(n)$$

$x^n+\cdots$的无穷级数称为x的幂级数. x与系数$a(n)$都是实数或复数. 对每一个幂级数有相应的收敛半径$r>0$，使得当$|x|<r$时，级数绝对收敛，而当$|x|>r$时级数发散.（半径r可以是$+\infty$.）

本节从另外的角度来考虑幂级数. 为区别微积分的普通的幂级数，我们称这种幂级数为形式幂级数. 在形式幂级数

的理论中，x从来不指定一个数值，且对收敛或发散的问题不感兴趣．感兴趣的是系数序列

(13) $(a(0), a(1), \cdots, a(n), \cdots)$.

我们研究形式幂级数完全可以归结为讨论这些系数序列，而系数序列又可看作含有分量$a(0)$, $a(1)$, …, $a(n)$, …的无穷维矢量．但对我们说来，展开(12)里的幂级数的系数比展开(13)里的向量分量更容易．符号x^n是确定n次项系数$a(n)$的位置的简便方法．系数$a(0)$称为级数的常数系数．

我们把形式幂级数看作是收敛的并在其上作代数运算．如果$A(x)$与$B(x)$是两个形式幂级数，

$$A(x)=\sum_{n=0}^{\infty} a(n)x^n \qquad 与 B(x)=\sum_{n=0}^{\infty} b(n)x^n \quad ,$$

我们规定：

相等：$A(x)=B(x)$

即$a(n)=b(n)$对所有的$n\geq 0$.

和：$A(x)+B(x)=\sum_{n=0}^{\infty}(a(n)+b(n))x^n$.

乘积：$A(x)B(x)=\sum_{n=0}^{\infty}c(n)x^n$，其中

(14) $C(n)=\sum_{k=0}^{n}a(k)b(n-k)$.

由(14)式确定的序列$\{c(n)\}$称为序列$\{a(n)\}$与$\{b(n)\}$的Cauchy乘积．读者容易验证这两种运算满足交换律与结合律，而乘积对加法满足分配律．用近世代数的话来讲，形式幂级数形成一个环，这个环对加法有零元并用0表示它，

$$0=\sum_{n=0}^{\infty}a(n)x^n，这里 a(n)=0 对所有的 n\geq 0,$$

对乘法有单位元我们用1来表示，

$$1=\sum_{n=0}^{\infty}a(n)x^n,$$

这里$a(0)=1$，$a(n)=0$对所有$n\geqslant1$.

如果从某项以后，形式幂级数的所有系数全为零，它就被称为形式多项式.

对每一个形式幂级数$A(x)=\sum_{n=0}^{\infty}a(n)x^n$，其常数项$a(0)\neq0$，有一个唯一确定的形式幂级数$B(x)=\sum_{n=0}^{\infty}b(n)x^n$，使得$A(x)B(x)=1$，$B(x)$的系数可由无穷的方程组的解来确定，

$$a(0)b(0)=1$$

$$a(0)b(1)+a(1)b(0)=0$$

$$a(0)b(2)+a(1)b(1)+a(2)b(0)=0$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

依次地可得$b(0)$，$b(1)$，$b(2)$，…，级数$B(x)$称为$A(x)$的逆并记为$A^{-1}(x)$或$\frac{1}{A(x)}$.

特殊的级数

$$A(x)=1+\sum_{n=1}^{\infty}a^nx^n$$

称为几何级数，其中a是任一实数或复数，它的逆是形式多项式

$$B(x)=1-ax,$$

换言之，我们有

$$\frac{1}{1-ax}=1+\sum_{n=1}^{\infty}a^nx^n.$$

2.16 数论函数的Bell级数

E.T.Bell利用形式幂级数去研究积性数论函数的性质.

定义 给定一个数论函数f与一个素数p，我们规定形式幂级数

$$f_p(x)=\sum_{n=0}^{\infty}f(p^n)x^n,$$

并称它是f关于模p的Bell级数.

当f是积性函数时，Bell级数特别有用.

定理2.24 唯一性定理. 令f与g是积性函数. 则

$f=g$ 当且仅当$f_p(x)=g_p(x)$ 对所的素数p.

证明 如果$f=g$，则对所有的p与所有的$n\geqslant 0$，有$f(p^n)=g(p^n)$，所以$f_p(x)=g_p(x)$. 反之，如果$f_p(x)=g_p(x)$对所有的p成立，则对所有的$n\geqslant 0$，$f(p^n)=g(p^n)$. 因f与g都是积性的且对所有的素数幂相等，于是对所有的正整数也相等，所以$f=g$.

本章前面介绍的一些积性数论函数的Bell级数容易确定.

例1. Möbius函数μ.因为$\mu(p)=-1$而对所有的$n\geqslant 2$，$\mu(P^n)=0$，所以有

$$\mu_p(x)=1-x.$$

例2. Euler函数φ. 因为对$n\geqslant 1$，$\varphi(p^n)=p^n-p^{n-1}$，所以我们有

$$\varphi_p(x)=1+\sum_{n=1}^{\infty}(p^n-p^{n-1})x^n$$

$$=\sum_{n=0}^{\infty}p^nx^n-x\sum_{n=0}^{\infty}p^nx^n$$

$$=(1-x)\sum_{n=0}^{\infty}p^n x^n=\frac{1-x}{1-px}.$$

例3. 完全积性函数．如果f是完全积性的，则对所有的$n\geqslant 0$，$f(p^n)=f(p)^n$，所以Bell级数$f_p(x)$是几何级数，

$$f_p(x)=\sum_{n=0}^{\infty}f(p)^n x^n=\frac{1}{1-f(p)x}.$$

特别，我们有下面的恒等函数I，单位函数u，幂函数N^α与Liouville函数λ的Bell级数：

$$I_p(x)=1.$$

$$u_p(x)=\sum_{n=0}^{\infty}x^n=\frac{1}{1-x}.$$

$$N_p^\alpha(x)=1+\sum_{n=1}^{\infty}p^{\alpha n}x^n=\frac{1}{1-P^\alpha x}.$$

$$\lambda_p(x)=\sum_{n=0}^{\infty}(-1)^n x^n=\frac{1}{1-x}.$$

2.17 Bell级数与Dirichlet乘积

下面的定理把Bell级数的乘积与Dirichlet乘积联系起来．

定理2.25 对任意两个数论函数f与g，令$h=f*g$，则对任意的素数p，我们有

$$h_p(x)=f_p(x)g_p(x).$$

证明 因为p^n的约数是1，p，p^2，…，p^n，所以有

$$h(p^n)=\sum_{d\mid p^n}f(d)g\left(\frac{p^n}{d}\right)=\sum_{k=0}^{n}f(p^k)g(p^{n-k}),$$

因为最后的和是序列$\{f(p^n)\}$与$\{g(p^n)\}$的Cauchy乘积，所以

证明完成.

例1. 因为$\mu^{\alpha}(n)=\lambda^{-1}(n)$，故$\mu^{\alpha}$对模p的Bell级数是

$$\mu_p^{\alpha}(x)=\frac{1}{\lambda_p(x)}=1+x.$$

例2. 因为$\sigma_\alpha=N^\alpha*u$，故σ_α对模p的Bell级数是

$$(\sigma_\alpha)_p(x)=N_p^\alpha(x)u_p(x)=\frac{1}{1-p^\alpha x}\cdot\frac{1}{1-x}$$

$$=\frac{1}{1-\sigma_\alpha(p)x+p^\alpha x^2}\ .$$

例3. 这个例子说明如何利用Bell级数去发现含有数论函数的等式. 令

$$f(n)=\alpha^{v(n)},$$

其中$v(1)=0$且$v(n)=k$当$n=p_1^{\alpha_1}\cdots p_x^{\alpha_x}$时. 那么f是积性的且它对模p的Bell级数是

$$f_p(x)=1+\sum_{n=1}^{\infty}2^{v(p^n)}x^n=1+\sum_{n=1}^{\infty}2x^n=1+\frac{2x}{1-x}$$

$$=\frac{1+x}{1-x},$$

于是

$$f_p(x)=\mu_p^2(x)u_p(x).$$

即 $f=\mu^2*u$ 或

$$2^{v(n)}=\sum_{d\mid n}\mu^2(d).$$

2.18 数论函数的导数

定义 对任一数论函数f我们定义它的导数f'是由下式给的数论函数:

$$f'(n)=f(n)\log n \qquad 对 n\geqslant 1.$$

例 因为对所有的 n，$I(n)\log n=0$，所以我们有 $I'=0$．又因对所有的n，$u(n)=1$，所以我们有 $u'(n)=\log n$，于是式子 $\sum_{d|n}\Lambda(d)=\log n$ 能写为

$$(15) \qquad \Lambda*u=u'.$$

这种概念的导数具有初等微积分中讨论的普通导数的许多性质．例如，如果乘积是Dirichlet乘积，则对和、乘积的微分的通常的规则也成立．

定理2.26 如果f与g是数论函数，我们有：

(a) $(f+g)'=f'+g'$.

(b) $(f*g)'=f'*g+f*g'$.

(c) $(f^{-1})'=-f'*(f*f)^{-1}$，规定 $f(1)\neq 0$.

证明 因为对所有的n，有 $(f+g)(n)=f(n)+g(n)$，所以立即得到(a)．

为证明(b)，我们利用等式 $\log n=\log d+\log\left(\frac{n}{d}\right)$，有

$$(f*g)'(n)=\sum_{d|n}f(d)g\left(\frac{n}{d}\right)\log n$$

$$=\sum_{d|n}f(d)\log d\,g\left(\frac{n}{d}\right)$$

$$+\sum_{d|n}f(d)g\left(\frac{n}{d}\right)\log\left(\frac{n}{d}\right)$$

$$=(f'*g)(n)+(f*g')(n).$$

为证明(c)，我们对公式 $I'=0$ 应用(b)．记住 $I=f*f^{-1}$，我们有

$$0=(f*f^{-1})'=f'*f^{-1}+f*(f^{-1})',$$

所以

$$f*(f^{-1})'=-f'*f^{-1}.$$

用f^{-1}去乘，得

$$(f^{-1})'=-(f'*f^{-1})*f^{-1}=-f'*(f^{-1}*f^{-1}).$$

但$f^{-1}*f^{-1}=(f*f)^{-1}$，所以(c)得证. □

2.19 Selberg等式

利用导数的概念我们能很快地导出Selberg等式，它常作为素数定理初等证明的起点.

定理2.27 Selberg等式. $n\geq 1$，我们有

$$\Lambda(n)\log n+\sum_{d\mid n}\Lambda(d)\Lambda\left(\frac{n}{d}\right)=\sum_{d\mid n}\mu(d)\log^2\frac{n}{d}.$$

证明 等式(15)说明$\Lambda*u=u'$. 对它求导数得，

$$\Lambda'*u+\Lambda*u'=u''.$$

或者，因为$u'=\Lambda*u$，所以

$$\Lambda'*u+\Lambda*(\Lambda*u)=u''.$$

用$\mu=u^{-1}$去乘，得

$$\Lambda'+\Lambda*\Lambda=u''*\mu,$$

这就是所求的等式.

第二章习题

1. 求整数n，使

(a) $\varphi(n)=\frac{n}{2}$；(b) $\varphi(n)=\varphi(2n)$；(c) $\varphi(n)=12$.

2. 对下列各条给出证明或举出一个反例：

(a) 若$(m, n)=1$，则$(\varphi(m), \varphi(n))=1$；

(b) 若n是复合数，则$(n, \varphi(n))>1$；

(c) 若m与n的素因数相同，则$n\varphi(m)=m\varphi(n)$。

3. 证明

$$\frac{n}{\varphi(n)}=\sum_{d\mid n}\frac{\mu^2(d)}{\varphi(d)}.$$

4. 证明$\varphi(n)>\frac{n}{6}$对最多只有8个不同素因数的所有的n成立。

5. 定义$V(1)=0$，对$n>1$，$V(n)$是n的不同素因数的个数．令$f=\mu*V$，证明$f(n)$为0或1．

6. 证明

$$\sum_{d^2\mid n}\mu(d)=\mu^2(n).$$

更一般，

$$\sum_{d^k\mid n}\mu(d)=\begin{cases}0 & \dfrac{m^k}{n}\text{对某个}m>1,\\ 1 & \text{其它}.\end{cases}$$

最后的和式在n的所有正约数d上展开，要求d^k也能整除n。

7. 令$\mu(p, d)$表示Möbius函数对p与d的最大公约数的值。证明，对每一个素数P，

$$\sum_{d\mid n}\mu(d)\mu(p,d)=\begin{cases}1 & n=1,\\ 2 & n=p^{\alpha}\quad \alpha\geqslant 1,\\ 0 & \text{其它}.\end{cases}$$

8. 证明

$$\sum_{d\mid n}\mu(d)\log^m d=0,$$

当$m\geqslant 1$且n有多于m个不同的素因数时．[提示：归纳法．]

9．如果x是实数，$x\geqslant 1$．令$\varphi(x,n)$表示$\leqslant x$的正整数中与n互素的数的个数．[记$\varphi(n,n)=\varphi(n)$]证明

$$\varphi(x,n)=\sum_{d\mid n}\mu(d)\frac{x}{d}\text{ 且 }\sum_{d\mid n}\varphi\left(\frac{x}{d},\frac{n}{d}\right)=[x].$$

在10.11.12题中，$d(n)$表示n的正约数的个数．

10．证明$\prod_{t\mid n}t=n^{\frac{d(n)}{2}}$．

11．证明$d(n)$是奇数当且仅当n是平方数．

12．证明$\sum_{t\mid n}d(t)^3=(\sum_{t\mid n}d(t))^2$．

13．Möbius反转公式的乘积形式．如果对所有的n，$f(n)>0$，且如果$a(n)$是实的，$a(1)\neq 0$．证明

$$g(n)=\prod_{d\mid n}f(d)^{a\left(\frac{n}{d}\right)}\text{当且仅当}f(n)=\prod_{d\mid n}g(d)^{b\left(\frac{n}{d}\right)}$$

其中$b=a^{-1}$是a的Dirichlet逆函数．

14．令$f(x)$对所有的$0\leqslant x<1$中有理数x有定义并令

$$F(n)=\sum_{k=1}^{n}f\left(\frac{k}{n}\right),\quad F^*(n)=\sum_{\substack{k=1\\(k,n)=1}}^{n}f\left(\frac{k}{n}\right).$$

(a) 证明$F^*=\mu*F$是μ与F的Dirichlet乘积．

(b) 利用(a)或其它方法证明$\mu(n)$是n次本原单位根的和：

$$\mu(n)=\sum_{\substack{k=1\\(k,n)=1}}^{n}e^{\frac{2\pi ik}{n}}.$$

15．令$\varphi_k(n)$表示$\leqslant n$的正整数中与n互素的数的k次方幂的和．注意$\varphi_0(n)=\varphi(n)$．利用14题或其它方法证明

$$\sum_{d\mid n}\frac{\varphi_k(d)}{d^k}=\frac{1^k+\cdots+n^k}{n^k}.$$

16．15题里公式的逆．对$n>1$

$$\varphi_1(n)=\frac{1}{2}n\varphi(n),$$

$$\varphi_2(n)=\frac{1}{3}n^2\varphi(n)+\frac{n}{6}\prod_{p\mid n}(1-p),$$

并推出$\varphi_3(n)$的相应的公式．

17．由

$$J_k(n)=n^k\prod_{p\mid n}(1-p^{-k})$$

定义的Jordan函数是Euler函数的一个推广．

(a) 证明

$$J_k(n)=\sum_{d\mid n}\mu(d)\left(\frac{n}{d}\right)^k,\ n^k=\sum_{d\mid n}J_k(d).$$

(b) 确定J_k的Bell级数．

18．证明，当$2^\alpha-1$是素数时，每一个形如$2^{\alpha-1}(2^\alpha-1)$的数是完全数．

19．证明，如果n是偶完全数，则$n=2^{\alpha-1}(2^\alpha-1)$，对某个$\alpha\geqslant2$．不知道奇完全数是否存在，但知道奇完全数的素因数的个数不会小于7．

20．令$p(n)$是$\leqslant n$的正整数中与n互素的诸数之积，证明

$$p(n)=n^{\varphi(n)}\prod_{d\mid n}\left(\frac{d!}{d^d}\right)^{\mu\left(\frac{n}{d}\right)}.$$

21．令$f(n)=[\sqrt{n}]-[\sqrt{n-1}]$，证明$f(n)$是积性的但不是完全积性的．

22．证明

$$\sigma_1(n)=\sum_{d\mid n}\varphi(d)\sigma_0\left(\frac{n}{d}\right),$$

并推导出一般的$\sigma_\alpha(n)$.

23. 证明下面的叙述或举出反例. 如果f是积性的，则$F(n)=\prod_{n\mid d}f(d)$也是积性的.

24. 令A(x)与B(x)都是形式幂级数. 如果A(x)B(x)是零级数，证明它至少有一个因子是零. 或者说，形式幂级数环没有零因子.

25. 令f是积性的，证明：

(a) $f^{-1}(n)=\mu(n)f(n)$对任意无平方因子数n成立.

(b) $f^{-1}(p^2)=f(p)^2-f(p^2)$对任意素数p成立.

26. 令f是积性的，证明，f是完全积性的当且仅当$f^{-1}(p^a)=0$对一切素数p与一切整数$a\geqslant 2$.

27. (a) 如果f是完全积性的，证明

$$f\cdot(g*h)=(f\cdot g)*(f\cdot h)$$

对所有的数论函数g与h成立，其中$f\cdot g$表示通常的乘积，$(f\cdot g)(n)=f(n)g(n)$

(b) 如果f是积性的且(a)里的关系式对$g=\mu$与$h=\mu^{-1}$成立，证明f是完全积性的.

28. (a) 如果f是完全积性的，证明$(f\cdot g)^{-1}=f\cdot g^{-1}$对每一个数论函数g成立，这里$g(1)\neq 0$.

(b) 如果f是积性的且对$g=\mu^{-1}$，(a)里的关系式成立，证明f是完全积性的.

29. 证明，存在一个积性数论函数g，使得

$$\sum_{k=1}^{n}f((k,n))=\sum_{d\mid n}f(d)g\left(\frac{n}{d}\right)$$

对每一个数论函数f成立．这里(k，n)是k与n的最大公约数．并利用此等式证明

$$\sum_{k=1}^{n}(k,\ n)\mu((k,\ n))=\mu(n).$$

30．令f是积性的并令g是任一数论函数，假设

(a) $f(p^{n+1})=f(p)f(p^n)-g(p)f(p^{n-1})$ 对所有素数p与所有$n\geqslant1$成立．证明，对每一素数p，f的Bell级数公式为

(b) $$f_p(x)=\frac{1}{1-f(p)x+g(p)x^{\alpha}}.$$

反之，证明，由(b)可推出(a)．

31．（30题的继续）如果g是完全积性的，证明，由30题的(a)可推出

$$f(m)f(n)=\sum_{d\mid(m,n)}g(d)f\left(\frac{mn}{d^2}\right),$$

其中和式在（m，n）的正约数上展开．[提示：首先讨论$m=p^a$、$n=p^b$的情形．]

32．证明

$$\sigma_a(m)\sigma_a(n)=\sum_{d\mid(m,n)}d^2\sigma_a\left(\frac{mn}{d^2}\right).$$

33．证明Liouville函数由公式

$$\lambda(n)=\sum_{d^2\mid n}\mu\left(\frac{n}{d^2}\right)$$

给定．

34．本题是定理2.16的一个替换证明，它说明积性函数的Dirichlet逆函数也是积性的．假设g是积性的并令$f=g^{-1}$．

(a) 证明如果p是素数，则对$k\geqslant 1$我们有

$$f(p^k)=-\sum_{t=1}^{k}g(p^t)f(p^{k-t}).$$

(b) 设h是唯一确定的积性函数，它与f同样定义在素数幂之上，$h*g$与恒等函数I同样定义在素数幂之上，试推出$h*g=I$，这说明$f=h$，所以f也是积性的.

35. 如果f与g是积性的且a与b是正整数，$a\geqslant b$. 证明由

$$h(n)=\sum_{d^a\mid n}f\left(\frac{n}{d^a}\right)g\left(\frac{n}{d^b}\right)$$

给定的函数也是积性的. 其中和式在n的约数d上展开，d满足$d^2\mid n$.

K阶Möbius函数.

如果$k\geqslant 1$，我们定义k阶Möbius函数μ_k如下：

$\mu_k(1)=1$

$\mu_k(n)=0$　　　若$p^{k+1}\mid n$对某个素数p.

$\mu_k(n)=(-1)^r$　　若$n=p_1^k\cdots p_r^k\prod_{i>r}p_i^{a_i}$，

$0\leqslant a_i<k$,

$\mu_k(n)=1$　　　其它.

或者说，如果n可以被某个素数的$k+1$次幂整除，则$\mu_k(n)$为零. 如果n的素因子分解式中恰有r个不同素数的k次幂，则$\mu_k(n)=(-1)^r$，其它情形的$\mu_k(n)$为1. 注意$\mu_1=\mu$就是通常的Möbius函数.

证明下列各题中函数μ_k的性质.

36. 如果$k\geqslant 1$，则$\mu_k(n^k)=\mu(n)$.

37. 每一个μ_k都是积性函数.

38. 如果$k\leqslant 2$，我们有

$$\mu_k(n)=\sum_{d^k|n}\mu_{k-1}\left(\frac{n}{d^k}\right)\mu_{k-1}\left(\frac{n}{d}\right).$$

39．如果$k\geqslant 1$，我们有

$$|\mu_k(n)|=\sum_{d^{k+1}|n}\mu(d).$$

40．对每一个素数p，μ_k的Bell级数为

$$(\mu_k)_p(x)=\frac{1-2x^k+x^{k+1}}{1-x}.$$

第三章　数论函数的平均值

3.1　引言

上一章讨论了各种各样的被数论函数$\mu(n)$，$\varphi(n)$、$\Lambda(n)$与除数函数$\sigma_\alpha(n)$满足的等式．现在我们研究这些函数与其它数论函数$f(n)$对于大值的n的特性．

例如，$d(n)$是n的约数的个数，这个函数经常为2（当n是素数时），但当n的约数的个数很多时，它的值可以是任意大．即当n不断增加时，$d(n)$的值是波动的．

在这种意义上看，很多数论函数波动而且对于大的n要确定这些特性常常是困难的．而研究算术平均数

$$\overline{f}(n)=\frac{1}{n}\sum_{k=1}^{n}f(k)$$

有时它更有效．平均值把波动变为平稳，所以希望平均值$\overline{f}(n)$能比$f(n)$更稳定是合理的．对于除数函数$d(n)$这是正确的．后面我们将证明，对于大的n，平均值$\overline{d}(n)$趋近于$\log n$，更准确地有

$$(1)\quad \lim_{n\to\infty}\frac{\overline{d}(n)}{\log n}=1,$$

这说明d(n)的平均阶是logn.

为了研究任意函数f的平均值，我们需要知道它的部分和$\sum_{k=1}^{n} f(k)$，用任一正实数x去代替上指标并讨论这种形式的代替和

$$\sum_{k\leq x} f(k)$$

有时是方便的，这里，指标k从1变到[x]是显然的，[x]是≤x的最大整数．如果$0<x<1$，则这个和是定的，我们指定它的值为0．我们的目的是确定作为x的函数的这个和的特性，特别是对于大的x.

对于除数函数我们将证明一个由Dirichlet在1849年得到的结果，它比(1)更强，即

$$(2)\quad \sum_{k\leq x} d(k) = x\log x + (2c-1)x + O(\sqrt{x}).$$

对所有$x\geq 1$成立．其中c是Euler常数，

$$(3)\quad C = \lim_{n\to\infty}\left(1+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{n}-\log n\right).$$

记号$O(\sqrt{x})$是一个还没有提到过的x的函数，它不比$\sqrt{x}$增大的更快，这是一个"大O"符号的例子，它的定义如下．

3.2 大O符号，函数的渐近等式

定义 如果对于所有的$x\geq a$，$g(x)>0$，我们写

$$f(x) = O(g(x)) \qquad (\text{读为}f(x)\text{是}g(x)\text{的大O})$$

表示对于$x\geq a$，商$\frac{f(x)}{g(x)}$是有界的．即存在一个常数$M>0$，使得

$$|f(x)|\leqslant Mg(x) \qquad \text{对所有的} x\geqslant a.$$

等式

$$f(x)=h(x)+O(g(x))$$

意即$f(x)-h(x)=O(g(x))$. 我们注意，对于$t\geqslant a$，$f(t)=O(g(t))$得出$\int_a^x f(t)dt=O\left(\int_a^x g(t)dt\right)$对$x\geqslant a$.

定义 如果

$$\lim_{x\to\infty}\frac{f(x)}{g(x)}=1,$$

我们称为当$x\to\infty$时，$f(x)$渐近于$g(x)$，并写为

$$f(x)\sim g(x) \qquad \text{当} x\to\infty.$$

例如，等式(2)即

$$\sum_{k\leqslant x}d(k)\sim x\log x \qquad \text{当} x\to\infty.$$

在等式(2)中，项$x\log x$称为这个和的渐近值，其余两项表示这个和以它的渐近值为近似值所造成的误差，如果用$E(x)$表示这个误差，则(2)式给出

$$(4)\quad E(x)=(2C-1)x+O(\sqrt{x}).$$

这也能改写为$E(x)=O(\sqrt{x})$，这个等式是正确的，但它不能表达(4)里更准确的情况. 等式(4)告诉我们$E(x)$的渐近值是$(2C-1)x$.

3.3 Euler求和公式

有时部分和的渐近值能由它与整数比较而得到. Euler求和公式对由近似值所产生的误差给出了一个准确的公式. 在这个公式里，$[t]$表示$\leqslant t$的最大整数.

定理3.1 Euler求和公式． 如果f在区间[y，x]上有连续导数f′，其中0＜y＜x，那么

$$(5)\quad \sum_{y<n\leqslant x} f(n)=\int_y^x f(t)dt+\int_y^x (t-[t])f'(t)dt$$
$$+f(x)([x]-x)-f(y)([y]-y).$$

证明．令m＝[y]，k＝[x]．对于在[y，x]里的整数n与n－1，我们有

$$\int_{n-1}^{n}[t]f'(t)dt=\int_{n-1}^{n}(n-1)f'(t)dt$$
$$=(n-1)\{f(n)-f(n-1)\}$$
$$=\{nf(n)-(n-1)f(n-1)\}$$
$$-f(n).$$

从n＝m＋1到n＝k求和，我们得

$$\int_m^k[t]f'(t)dt=\sum_{n=m+1}^{k}\{nf(n)-(n-1)f(n-1)\}$$
$$-\sum_{y<n\leqslant x}f(n)$$
$$=kf(k)-mf(m)-\sum_{y<n\leqslant x}f(n),$$

于是有

$$(6)\quad \sum_{y<n\leqslant x}f(n)=-\int_m^k[t]f'(t)dt+kf(k)-mf(m)$$
$$=-\int_y^x[t]f'(t)dt+kf(x)-mf(y).$$

由分部积分得

$$\int_y^x f(t)dt=xf(x)-yf(y)-\int_y^x tf'(t)dt,$$

此式联同(6)式即得(5)式． □

3.4 几个基本渐近公式

下面的定理给出一批渐近公式，它们是Euler求和公式的简单的推论．在(a)里，C是(3)式里定义的Euler常数．在(b)里，$\zeta(s)$表示Riemam zeta函数，其定义为

$$\zeta(s)=\sum_{n=1}^{\infty}\frac{1}{n^s}\qquad s>1,$$

与

$$\zeta(s)=\lim_{x\to\infty}\left(\sum_{n\leqslant x}\frac{1}{n^s}-\frac{x^{1-s}}{1-s}\right)\qquad 0<S<1.$$

定理3.2　如果$x\geqslant 1$，我们有

(a) $\displaystyle\sum_{n\leqslant x}\frac{1}{n}=\log x+C+0\left(\frac{1}{x}\right).$

(b) $\displaystyle\sum_{n\leqslant x}\frac{1}{n^s}=\frac{x^{1-s}}{1-s}+\zeta(s)+0(x^{-s})$若$s>0$，$s\neq 1$；

(c) $\displaystyle\sum_{n>x}\frac{1}{n^s}=0(x^{1-s})$　　如果$s>1$．

(d) $\displaystyle\sum_{n\leqslant x}n^{\alpha}=\frac{x^{\alpha+1}}{\alpha+1}+0(x^{\alpha})$　　如果$\alpha\geqslant 0$．

证明　对于(a)，在Euler求和公式里我们取$f(t)=\frac{1}{t}$，得

$$\sum_{n\leqslant x}\frac{1}{n}=\int_1^x\frac{dt}{t}-\int_1^x\frac{t-[t]}{t^2}dt+1-\frac{x-[x]}{x}$$

$$=\log x-\int_1^x\frac{t-[t]}{t^2}dt+1+0\left(\frac{1}{x}\right)$$

$$=\log x+1-\int_1^{\infty}\frac{t-[t]}{t^2}dt$$

$$+\int_x^{\infty}\frac{t-[t]}{t}dt+0\left(\frac{1}{x}\right).$$

广义积分$\int_1^{\infty}(t-[t])dt$是存在的，因为它小于$\int_1^{\infty}t^{-2}dt$，还有

$$0\leqslant\int_x^{\infty}\frac{t-[t]}{t^2}dt\leqslant\int_x^{\infty}\frac{1}{t^2}dt=\frac{1}{x},$$

上面的等式变为

$$\sum_{n\leqslant x}\frac{1}{n}=\log x+1-\int_1^{\infty}\frac{t-[t]}{t^2}dt+0\left(\frac{1}{x}\right)$$

这就是(a)的证明，(a)中

$$C=1-\int_1^{\infty}\frac{t-[t]}{t^2}dt.$$

令(a)中$x\to\infty$，得

$$\lim_{x\to\infty}\left(\sum_{n\leqslant x}\frac{1}{n}-\log x\right)=1-\int_1^{\infty}\frac{t-[t]}{t^2}dt,$$

所以C也等于Euler常数.

为证明(b)，我们有类似的理由取$f(x)=x^{-s}$，其中$s>0$，$s\neq1$．由Euler求和公式得

$$\sum_{n\leqslant x}\frac{1}{n^s}=\int_1^x\frac{dt}{t^s}-s\int_1^x\frac{t-[t]}{t^{s+1}}dt+1-\frac{x-[x]}{x^s}$$

$$=\frac{x^{1-s}}{1-s}-\frac{1}{1-s}+1-s\int_1^{\infty}\frac{t-[t]}{t^{s+1}}dt$$

$$+0(x^{-s}).$$

因此

$$\sum_{n\leqslant x}\frac{1}{n^s}=\frac{x^{1-s}}{1-s}+C(s)+0(x^{-s}),$$

其中

$$C(s)=1-\frac{1}{1-s}-\int_1^{\infty}\frac{t-[t]}{t^{s+1}}dt.$$

如果$s>1$，(7)左端趋于$\zeta(s)$，当$x\to\infty$时．而x^{1-s}与x^{-s}均趋于0．于是当$s>1$时，$C(s)=\zeta(s)$．当$0<s<1$时，$x^{-s}\to 0$．(7)式说明

$$\lim_{x\to\infty}\left(\sum_{n\leqslant x}\frac{1}{n^s}-\frac{x^{1-s}}{1-s}\right)=C(s).$$

因此，如果$0<s<1$，$C(s)$也等于$\zeta(s)$．这证明了(b)．

为证明(c)，我们利用(b)，取$s>1$，得

$$\sum_{n>x}\frac{1}{n^s}=\zeta(s)-\sum_{n\leqslant x}\frac{1}{n^s}=\frac{x^{s-1}}{s-1}+0(x^{-s})$$
$$=0(x^{1-s}),$$

这因为$x^{-s}\leqslant x^{1-s}$．

最后，为证明(d)我们再一次利用Euler求和公式以及$f(t)=t^{\alpha}$，得

$$\sum_{n\leqslant x}n^{\alpha}=\int_1^x t^{\alpha}dt+\alpha\int_1^x t^{\alpha-1}(t-[t])dt+1$$
$$-(x-[x])x^{\alpha}$$
$$=\frac{x^{\alpha+1}}{\alpha+1}-\frac{1}{\alpha+1}+0\left(\alpha\int_1^x t^{\alpha-1}dt\right)+0(x^{\alpha})$$
$$=\frac{x^{\alpha+1}}{\alpha+1}+0(x^{\alpha}).$$

3.5 d(n)的平均阶

本节我们推导出除数函数$d(n)$的部分和的Dirichlet渐

近公式。

定理3.3　对所有$x\geqslant 1$，我们有

$$(8)\quad \sum_{n\leqslant x} d(n)=x\log x+(2C-1)x+0(\sqrt{x}),$$

其中C是Euler常数.

证明　因为$d(n)=\sum_{d\mid n}1$，所以我们有

$$\sum_{n\leqslant x} d(n)=\sum_{n\leqslant x}\sum_{d\mid n}1,$$

这是个在n与d上展开的双重求和式．因为$d|n$，所以我们写$n=qd$，并对所有的q，d，$qd\leqslant x$展开这个和式，于是有

$$(9)\quad \sum_{n\leqslant x} d(n)=\sum_{\substack{q,d\\ qd\leqslant x}}1.$$

这说明和式能在qd平面内的一些格点上展开，如图3.1所示．（格点就是坐标为整数的点．）双曲线$qd=n$上有格点，所以(9)式里的和就是计算对应于$n=1$、$2\cdots$，$[x]$的双曲线$qd=n$上的格点的个数．对于每一个固定的$d\leqslant x$，我们首先计算水平线段$1\leqslant q\leqslant\frac{x}{d}$上的格点的个数，然后在所有的$d\leqslant x$上求和，因而(9)式变为

$$(10)\quad \sum_{n\leqslant x} d(n)=\sum_{d\leqslant x}\sum_{q\leqslant\frac{x}{d}}1.$$

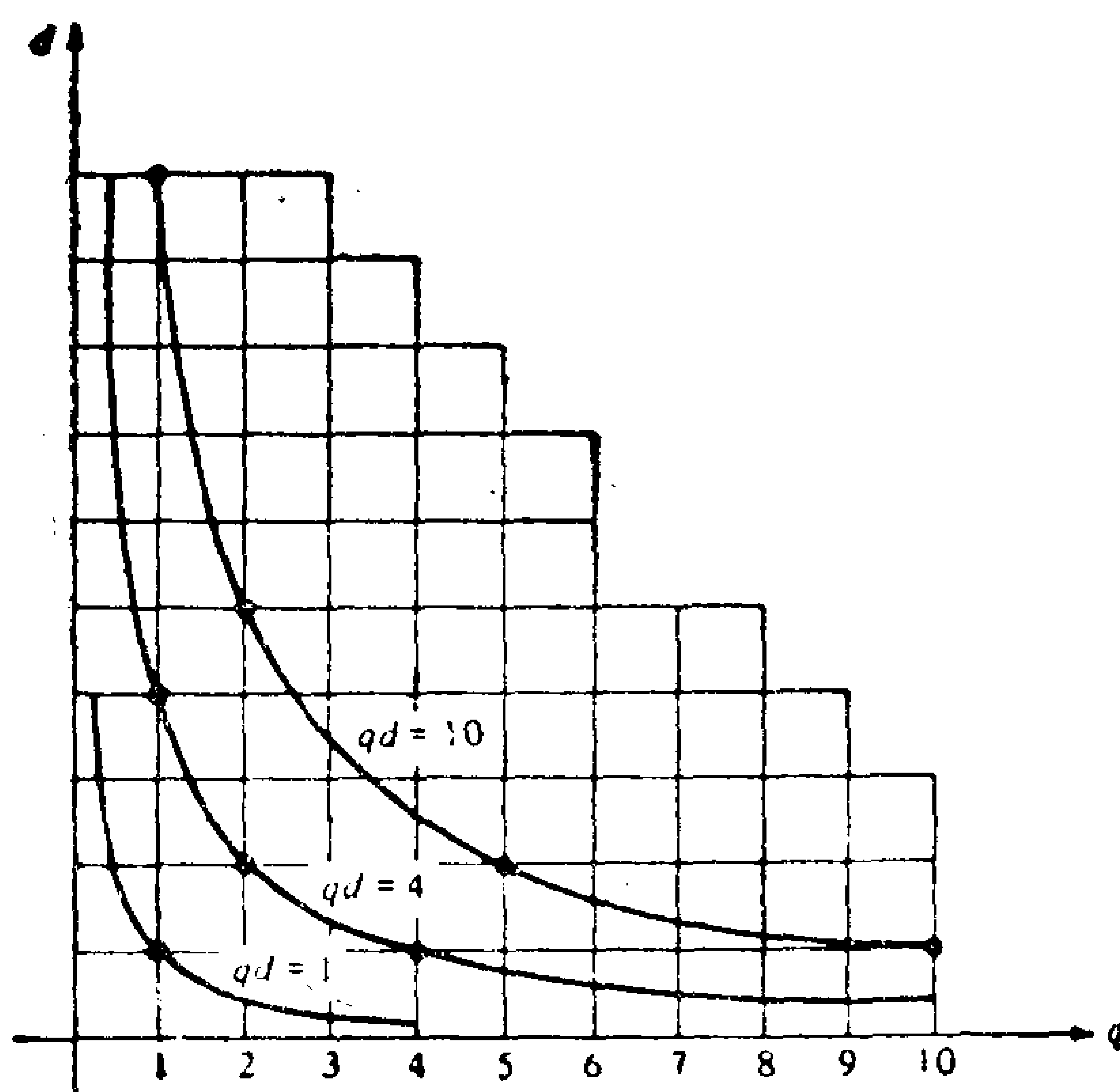
现在我们利用定理3.2的(d)，并令$\alpha=0$，得

$$\sum_{q\leqslant\frac{x}{d}}1=\frac{x}{d}+0(1).$$

利用此式与定理3.2(a)，我们得

$$\sum_{n\leqslant x} d(n)=\sum_{d\leqslant x}\left\{\frac{x}{d}+0(1)\right\}=x\sum_{d\leqslant x}\frac{1}{d}+0(x)$$

$$=x\left\{\log x+c+0\left(\frac{1}{x}\right)\right\}+0(x)$$



（图3.1）

$$= x\log x + O(x).$$

这是(8)的一个弱的形式，由此得出

$$\sum_{n\leq x} d(n) \sim x\log x \qquad 当x\to\infty时.$$

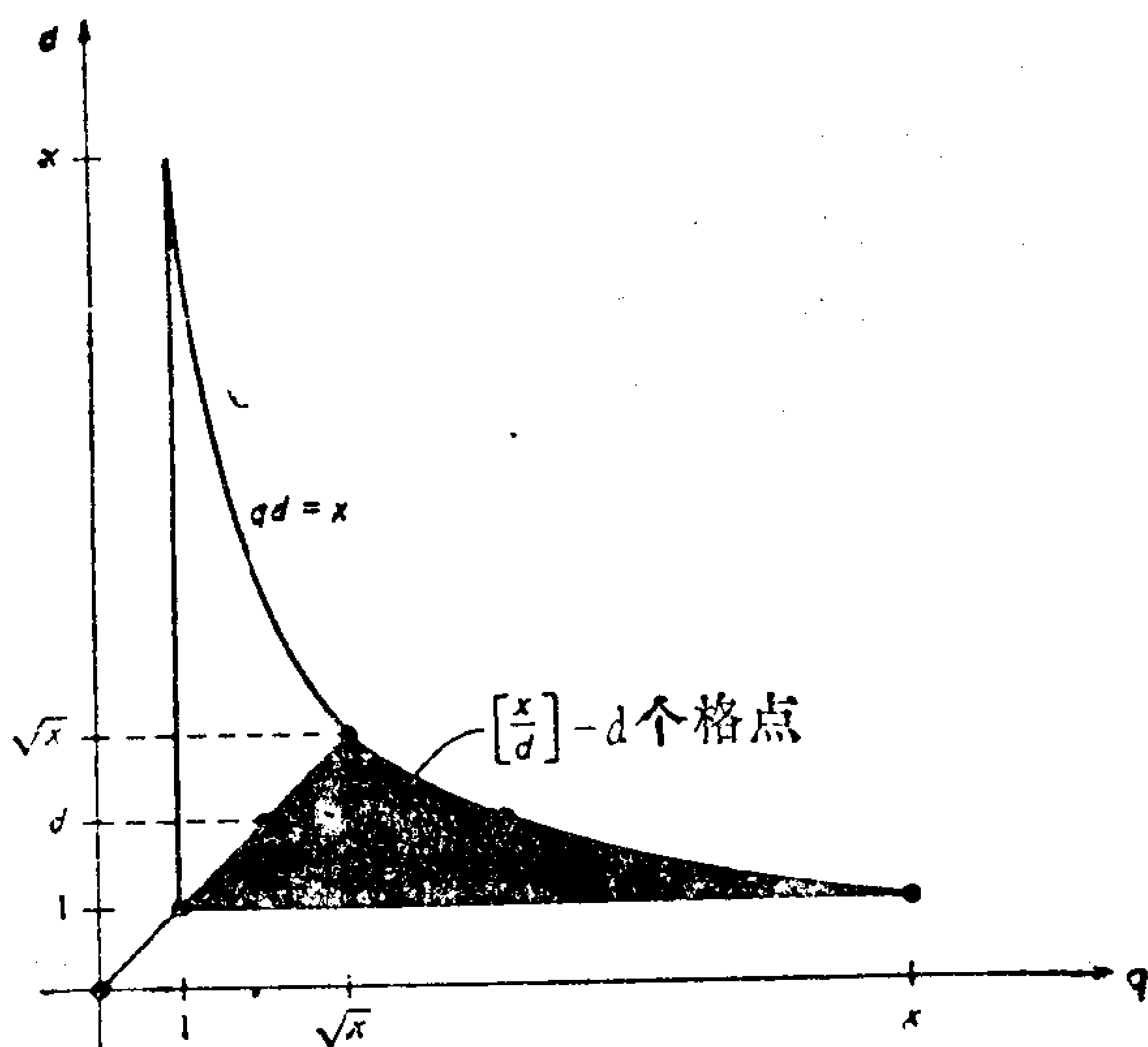
这给出d(n)的平均阶为logn.

为了证明更精确的公式(8)，我们回到和式(9)，它计算在一个双曲线区域内格点的个数并利用它在直线q＝d附近区域内的对称性．在这个区域内格点的总数等于在直线q＝d下面的格点数的2倍加上平分线线段上的格点数．

借助于图3.2，我们看出

$$\sum_{n\leq x} d(n) = 2\sum_{d\leq\sqrt{x}}\left\{\left[\frac{x}{d}\right] - d\right\} + [\sqrt{x}].$$

于是我们利用$[y] = y + O(1)$与定理3.2的(a)与(d)得



（图3.2）

$$\sum_{n\leqslant x} d(n)=2\sum_{d\leqslant\sqrt{x}}\left\{\frac{x}{d}-d-0(1)\right\}+0(\sqrt{x})$$

$$=2x\sum_{d\leqslant\sqrt{x}}\frac{1}{d}-2\sum_{d\leqslant\sqrt{x}}d+0(\sqrt{x})$$

$$=2x\left\{\log\sqrt{x}+C+0\left(\frac{1}{\sqrt{x}}\right)\right\}$$

$$-2\left\{\frac{x}{2}+0(\sqrt{x})\right\}+0(\sqrt{x})$$

$$=x\log x+(2C-1)x+0(\sqrt{x}).$$

Dirichlet公式的证明完成.

注：误差项$0(\sqrt{x})$还能改进.1903年Voronoi证明误差是$0(x^{\frac{1}{3}}\log x)$;1922年Van der Lorput改进为$0(x^{\frac{33}{100}})$，到目前为止最好的估计是

$O(x^{\frac{12}{37}+\varepsilon})$对每一个$\varepsilon>0$，它是由Kolesnik[35]在1969年得到的. 使误差项$O(x^\theta)$的所有θ的下确界确定的问题与Dirichlet除数问题一样是一个尚未解决的问题. 1915年Hardy与Landau证明$\theta\geqslant\frac{1}{4}$.

3.6 除数函数$\sigma_\alpha(n)$的平均阶

在定理3.3里已讨论过$\alpha=0$的情形. 下面我们讨论实数$\alpha>0$的情形并特别地讨论$\alpha=1$的情况.

定理3.4 **对所有的$x\geqslant1$，我们有**

$$(11)\quad \sum_{n\leqslant x}\sigma_1(n)=\frac{1}{2}\zeta(2)x^2+O(x\log x).$$

注：能够证明$\zeta(2)=\frac{\pi^2}{6}$，所以(11)表明$\sigma_1(n)$的平均阶是$\frac{\pi^2 n}{12}$.

证明　与定理3.3的弱的形式的推导相类似，我们有

$$\begin{aligned}\sum_{n\leqslant x}\sigma_1(n)&=\sum_{n\leqslant x}\sum_{q\mid n}q=\sum_{\substack{q,d\\ qd\leqslant x}}q=\sum_{d\leqslant x}\sum_{q\leqslant\frac{x}{d}}q\\&=\sum_{d\leqslant x}\left\{\frac{1}{2}\left(\frac{x}{d}\right)^2+O\left(\frac{x}{d}\right)\right\}\\&=\frac{x^2}{2}\sum_{d\leqslant x}\frac{1}{d^2}+O\left(x\sum_{d\leqslant x}\frac{1}{d}\right)\\&=\frac{x^2}{2}\left\{-\frac{1}{x}+\zeta(2)+O\left(\frac{1}{x^2}\right)\right\}\\&\quad+O(x\log x)\\&=\frac{1}{2}\zeta(2)x^2+O(x\log x).\end{aligned}$$

其中我们利用了定理3.2的(a)与(b). □

定理3.5 **如果$x\geqslant1$且$\alpha>0$，$\alpha\neq1$，我们有**

$$\sum_{n\leqslant x}\sigma_\alpha(n)=\frac{\zeta(\alpha+1)}{\alpha+1}x^{\alpha+1}+O(x^\beta),$$

其中$\beta=\max\{1, \alpha\}$.

证明　这一次我们利用定理3.2的(b)与(d)得

$$\sum_{n\leqslant x}\sigma_\alpha(n)=\sum_{n\leqslant x}\sum_{q\mid n}q^\alpha=\sum_{d\leqslant x}\sum_{q\leqslant\frac{x}{d}}q^\alpha$$

$$=\sum_{d\leqslant x}\left\{\frac{1}{\alpha+1}\left(\frac{d}{x}\right)^{\alpha+1}+O\left(\frac{x^\alpha}{d^\alpha}\right)\right\}$$

$$=\frac{x^{\alpha+1}}{\alpha+1}\sum_{d\leqslant x}\frac{1}{d^{\alpha+1}}+O\left(x^\alpha\sum_{d\leqslant x}\frac{1}{d^\alpha}\right)$$

$$=\frac{x^{\alpha+1}}{\alpha+1}\left\{\frac{x^{-\alpha}}{-\alpha}+\zeta(\alpha+1)+O(x^{-\alpha-1})\right\}$$

$$+O\left(x^\alpha\left\{\frac{x^{1-\alpha}}{1-\alpha}+\zeta(\alpha)+O(x^{-\alpha})\right\}\right)$$

$$=\frac{\zeta(\alpha+1)}{\alpha+1}x^{\alpha+1}+O(x)+O(1)+O(x^\alpha)$$

$$=\frac{\zeta(\alpha+1)}{\alpha+1}x^{\alpha+1}+O(x^\beta),$$

其中$\beta=\max\{1, \alpha\}$.　□

为了求对于负数α的$\sigma_\alpha(n)$的平均阶，我们写$\alpha=-\beta$，其中$\beta>0$.

定理3.6　如果$\beta>0$，令$\delta=\max\{0, 1-\beta\}$，则当$x>1$时，我们有

$$\sum_{n\leqslant x}\sigma_\beta(n)=\zeta(\beta+1)+O(x^\delta)\quad 若\beta\neq1,$$

$$=\zeta(2)x+O(\log x)\quad 若\beta=1.$$

证明　我们有

$$\sum_{n\leqslant x}\sigma_{-\beta}(n)=\sum_{n\leqslant x}\sum_{d\mid n}\frac{1}{d^\beta}=\sum_{d\leqslant x}\frac{1}{d^\beta}\sum_{q\leqslant\frac{x}{d}}1$$

$$= \sum_{d \le x} \frac{1}{d^\beta}\left\{\frac{x}{d} + O(1)\right\}$$

$$= x\sum_{d \le x} \frac{1}{d^{\beta+1}} + O\left(\sum_{d \le x} \frac{1}{d^\beta}\right).$$

最后一项当$\beta=1$时是$O(\log x)$，当$\beta \neq 1$时是$O(x^\delta)$，因为

$$x\sum_{d \le x} \frac{1}{d^{\beta+1}} = \frac{x^{1-\beta}}{-\beta} + \zeta(\beta+1)x + O(x^{-\beta})$$

$$= \zeta(\beta+1)x + O(x^{1-\beta}),$$

所以证明完成. □

3.7 $\varphi(n)$的平均阶

Euler函数的部分和的渐近公式包含有级数的和

$$\sum_{n=1}^{\infty} \frac{\mu(n)}{n^2},$$

这个级数绝对收敛，因为它不超过$\sum_{n=1}^{\infty} n^{-2}$. 下一章我们将要证明

$$(12) \quad \sum_{n=1}^{\infty} \frac{\mu(n)}{n^2} = \frac{1}{\zeta(2)} = \frac{6}{\pi^2}.$$

先暂时假设这是成立的，我们有

$$\sum_{n \le x} \frac{\mu(n)}{n^2} = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^2} - \sum_{n > x} \frac{\mu(n)}{n^2}$$

$$= \frac{6}{\pi^2} + O\left(\sum_{n > x} \frac{1}{n^2}\right)$$

$$= \frac{6}{\pi^2} + O\left(\frac{1}{x}\right),$$

这是根据定理3.2的(c)． 利用此结果立即可得 $\varphi(n)$的平均阶．

定理3.7　对于$x>1$，我们有

$$(13)\quad \sum_{n\leq x}\varphi(n)=\frac{3}{\pi^2}x^2+O(x\log x),$$

所以 $\varphi(n)$的平均阶是$\frac{3n}{\pi^2}$.

证明　与除数函数的方法类似，首先有

$$\varphi(n)=\sum_{d\mid n}\mu(d)\frac{n}{d}.$$

得到

$$\begin{aligned}\sum_{n\leq x}\varphi(n)&=\sum_{n\leq x}\sum_{d\mid n}\mu(d)\frac{n}{d}=\sum_{\substack{q,d\\ qd\leq x}}\mu(d)q\\&=\sum_{d\leq x}\mu(d)\sum_{q\leq x/d}q\\&=\sum_{d\leq x}\mu(d)\left\{\frac{1}{2}\left(\frac{x}{d}\right)^2+O\left(\frac{x}{d}\right)\right\}\\&=\frac{1}{2}x^2\sum_{d\leq x}\frac{\mu(d)}{d^2}+O\left(x\sum_{d\leq x}\frac{1}{d}\right)\\&=\frac{1}{2}x^2\left\{\frac{6}{\pi^2}+O\left(\frac{1}{x}\right)\right\}+O(x\log x)\\&=\frac{3}{\pi^2}x^2+O(x\log x).\end{aligned}$$

□

3.8　对于由原点可见的格点分布的应用

$\varphi(n)$的部分和的渐近公式的一个有趣的应用是由原点可见的格点分布定理．

定义 两个格点p与称θ为是相互可见的，如果连结它们的直线段上除去端点p与θ之外不含其它格点.

定理3.8 两个格点(a，b)与(m，n)是相互可见的当且仅当a－m与b－n互素.

证明 显然(a，b)与(m，n)是相互可见的当且仅当(a－m，b－n)是从原点可见的，于是当(m，n)＝(0，0)时，定理是成立的.

假设(a，b)是由原点可见的，并令d＝(a，b)，我们证明d＝1，如果d＞1，则有$a=da'$，$b=db'$且格点(a', b')在连接(0，0)与(a，b)的直线段上，这个矛盾证明了d＝1.

反之，设(a，b)＝1，如果有一个格点(a', b')在联结(0，0)与(a，b)的直线段上，则有

$$a'=ta,\ b'=tb \quad 这里0<t<1,$$

因此t是有理数，所以$t=\frac{r}{s}$，这里r，s是正整数且(r，s)＝1，于是

$$sa'=ar,\ sb'=br,$$

所以$s|ar$，$s|br$. 但(s，r)＝1，所以$s|a$，$s|b$而(a，b)＝1. 所以s＝1，这与不等式$0<t<1$矛盾. 因此格点(a，b)是由原点可见的. □

有无穷多个由原点可见的格点. 自然要问，它们在平面上的分布情况怎样.

考虑在xy平面上由不等式$|x|\leqslant r$，$|y|\leqslant r$确定的大的方形区域. 令N(r)表示在这个方形内的格点的个数，并令$N'(r)$表示由原点可见的格点的个数. 商$\frac{N'(r)}{N(r)}$是度量这个方形内由原点可见的格点的分数. 下一个定理说明这个分

数随r→∞而趋于一个极限，我们称这个极限为由原点可见的格点的密度.

定理3.9　由原点可见的格点集合的密度为$\frac{6}{\pi^2}$.

证明　我们将证明

$$\lim_{r\to\infty}\frac{N'(r)}{N(r)}=\frac{6}{\pi^2}.$$

与原点最近的八个格点都是由原点可见的.（见图3.3），根据对称性，我们看到N′(r)等于8再加上区域

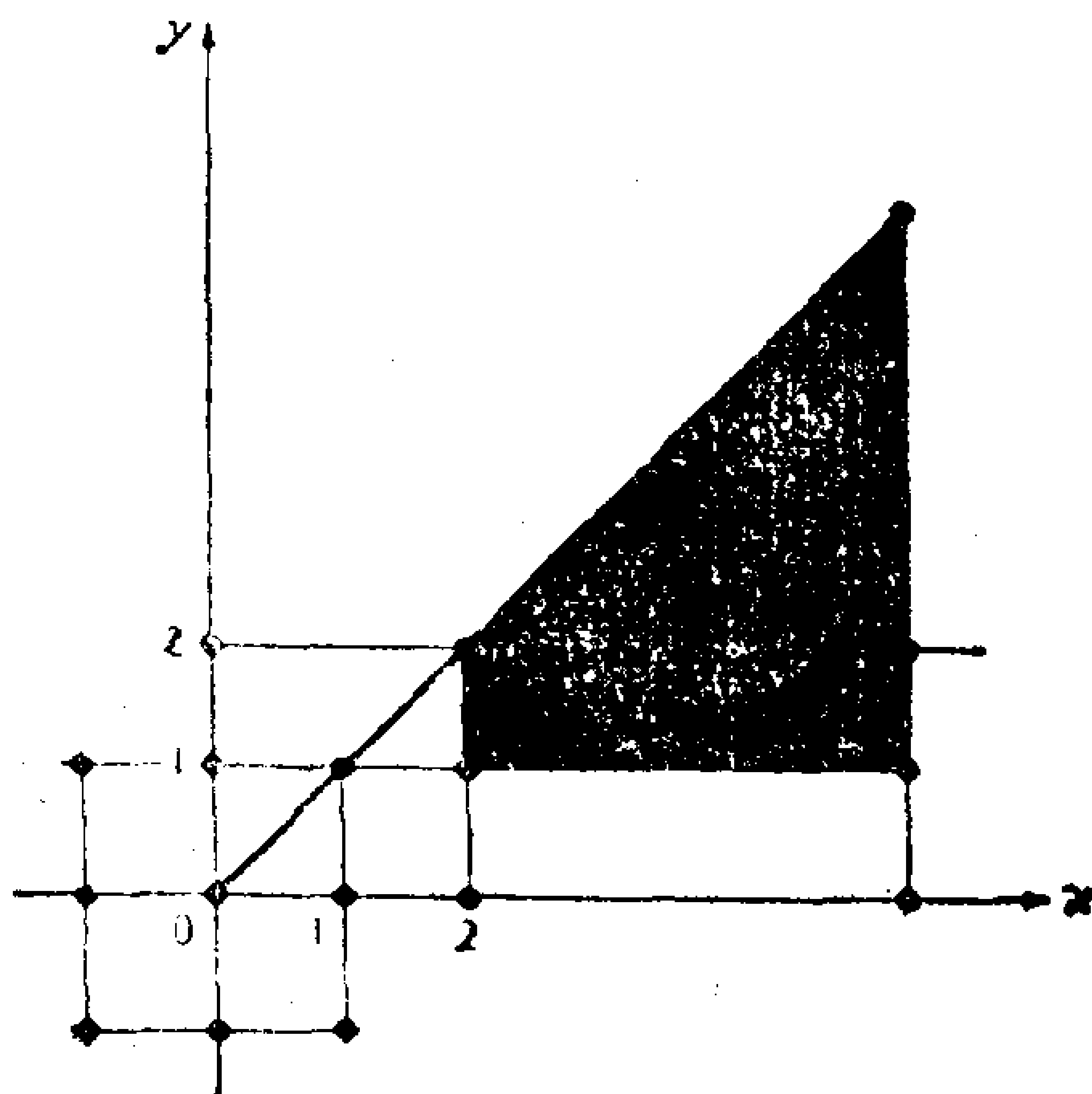
$$\{(x,\ y):2\leqslant x\leqslant r,\ 1\leqslant y\leqslant r\}$$

（图3.3的阴影部分）内由原点可见的格点数的8倍，即

$$N'(r)=8+8\sum_{2\leqslant n\leqslant r}\ \sum_{\substack{1\leqslant m<n\\(m,n)=1}}1=8\sum_{1\leqslant n\leqslant r}\varphi(n).$$

利用定理3.7，我们有

$$N'(r)=\frac{24}{\pi^2}r^2+O(r\log r).$$



（图3.3）

但是，在这个方形内格点的总数是

$$N(r)=(2[r]+1)^2=(2r+O(1))^2=4r^2+O(r),$$

所以

$$\frac{N'(r)}{N(r)}=\frac{\frac{24}{\pi^2}r^2+O(r\log r)}{4r^2+O(r)}$$

$$=\frac{\frac{6}{\pi^2}+O\left(\frac{\log r}{r}\right)}{1+O\left(\frac{1}{r}\right)},$$

当$r\to\infty$时，我们得到$\frac{N'(r)}{N(r)}\longrightarrow\frac{6}{\pi^2}$. □

注：定理3.9的结果有时也描述为，随意挑选的格点中由原点可见的格点的概率是$\frac{6}{\pi^2}$、或者说，任意挑选两个整数a与b互素的概率是$\frac{6}{\pi^2}$.

3.9 $\mu(n)$与$\Lambda(n)$的平均阶

$\mu(n)$与$\Lambda(n)$的平均阶的确定比$\varphi(n)$与除数函数的平均阶的确定要困难得多. 大家知道，$\mu(n)$平均阶为0，$\Lambda(n)$的平均阶为1，即

$$\lim_{x\to\infty}\frac{1}{x}\sum_{n\leqslant x}\mu(n)=0,\quad \lim_{x\to\infty}\frac{1}{x}\sum_{n\leqslant x}\Lambda(n)=1.$$

但是其证明是不容易的. 下一章我们将证明这两个结果等价于素数定理：

$$\lim_{x\to\infty}\frac{\pi(x)\log x}{x}=1,$$

其中$\pi(x)$是$\leqslant x$的素数的个数.

在这一章我们将得到包括$\mu(n)$与$\Lambda(n)$的一些基本等

式，它们在素数分布的研究中将要用到，这些等式将由任意的数论函数f与g以及它们的Dirichlet乘积$f*g$的部分和的一般公式推出.

3.10 Dirichlet乘积的部分和

定理3.10 如果$h=f*g$，令

$$H(x)=\sum_{n\leq x}h(n),\quad F(x)=\sum_{n\leq x}f(n)\text{与}$$
$$G(x)=\sum_{n\leq x}g(n),$$

则有

$$(14)\quad H(x)=\sum_{n\leq x}f(n)G\left(\frac{x}{n}\right)=\sum_{n\leq x}g(n)F\left(\frac{x}{n}\right).$$

证明 令

$$U(x)=\begin{cases}0 & 0<x<1\\ 1 & x\geq 1,\end{cases}$$

则$F=f\circ U$，$G=g\circ U$. 我们利用关于运算$\circ$与$*$的结合律，有

$$f\circ G=f\circ(g\circ U)=(f*g)\circ U=H,$$
$$g\circ F=g\circ(f\circ U)=(g*f)\circ U=H.$$

证明完成. □

如果对所有的n，$g(n)=1$，则$G(x)=[x]$且(14)式为我们给出下面的推论.

定理3.11 如果$F(x)=\sum_{n\leq x}f(n)$，则有

$$(15)\quad \sum_{n\leq x}\sum_{d\mid n}f(d)=\sum_{n\leq x}f(n)\left[\frac{x}{n}\right]=\sum_{n\leq x}F\left(\frac{x}{n}\right).$$

3.11 对$\mu(n)$与$\Lambda(n)$的应用

现在我们在定理3.11里取$f(n)=\mu(n)$与$\Lambda(n)$，可得到下列性质，这些性质在素数的分布的研究中将会用到.

定理3.12 对$x\geq 1$，我们有

(16) $\sum_{n\leq x}\mu(n)\left[\frac{x}{n}\right]=1$

与

(17) $\sum_{n\leq x}\Lambda(n)\left[\frac{x}{n}\right]=\log[x]!$.

证明 由(15)式，我们有

$$\sum_{n\leq x}\mu(n)\left[\frac{x}{n}\right]=\sum_{n\leq x}\sum_{d\mid n}\mu(d)=\sum_{n\leq x}\left[\frac{1}{n}\right]=1,$$

$$\sum_{n\leq x}\Lambda(n)\left[\frac{x}{n}\right]=\sum_{n\leq x}\sum_{d\mid n}\Lambda(d)$$

$$=\sum_{n\leq x}\log n=\log[x]! \qquad \square$$

注：定理3.12里的和可认为是$\mu(n)$与$\Lambda(n)$的平均重量.

在定理4.16里我们将证明素数定理，该定理随级数$\sum_{n=1}^{\infty}\frac{\mu(n)}{n}$收敛且和为零立即可得. 利用(16)式我们能证明这个级数的部分和有界.

定理3.13 对所有的$x\geq 1$，我们有

(18) $\left|\sum_{n\leq x}\frac{\mu(n)}{n}\right|\leq 1$,

且仅当$x<2$时，等号成立.

证明 如果$x<2$，则和式里仅有一项$\mu(1)=1$. 现在假设$x\geq 2$，对每一个实数y，令$\{y\}=y-[y]$，则有

$$1=\sum_{n\leqslant x}\mu(n)\left[\frac{x}{n}\right]=\sum_{n\leqslant x}\mu(n)\left(\frac{x}{n}-\left\{\frac{x}{n}\right\}\right)$$
$$=x\sum_{n\leqslant x}\frac{\mu(n)}{n}-\sum_{n\leqslant x}\mu(n)\left\{\frac{x}{n}\right\}.$$

因为$0\leqslant\{y\}<1$，这得出

$$x\left|\sum_{n\leqslant x}\frac{\mu(n)}{n}\right|=\left|1+\sum_{n\leqslant x}\mu(n)\left\{\frac{x}{n}\right\}\right|$$
$$\leqslant 1+\sum_{n\leqslant x}\left\{\frac{x}{n}\right\}$$
$$=1+\{x\}+\sum_{2\leqslant n\leqslant x}\left\{\frac{x}{n}\right\}$$
$$<1+\{x\}+[x]-1=x.$$

用x去除，我们得(18)式中严格的不等号. □

下面我们回到定理3.12的等式(17).

$$(17)\quad \sum_{n\leqslant x}\Lambda(n)\left[\frac{x}{n}\right]=\log[x]!$$

并利用它去确定素数的方幂，这个素数要整除一个阶乘.

定理3.14 Legendre等式．对每一个$x\geqslant1$，我们有

$$(19)\quad [x]!=\prod_{p\leqslant x}p^{\alpha(p)}$$

其中乘积号在$\leqslant x$的所有素数上展开，并且

$$(20)\quad \alpha(p)=\sum_{m=1}^{\infty}\left[\frac{x}{p^m}\right].$$

注：$\alpha(p)$的和式是有限的，因为对于$p>x$，$\frac{[x]}{p^m}=0$.

证明　如果n不是一个素数的方幂，则有$\Lambda(n)=0$，且$\Lambda(p^m)=\log p$，所以，

$$\log[x]!=\sum_{n\leqslant x}\Lambda(n)\left[\frac{x}{n}\right]=\sum_{p\leqslant x}\sum_{m=1}^{\infty}\left[\frac{x}{p^m}\right]\log p$$
$$=\sum_{p\leqslant x}\alpha(p)\log p,$$

其中$\alpha(p)$由(20)式给出，最后的和式就是(19)两边的对数式．所以证明完成． □

下面我们利用Euler求和公式去确定$\log[x]!$的渐近公式．

定理3.15　如果$x\geq 2$，我们有

$$(21)\quad \log[x]! = x\log x - x + O(\log x),$$

于是还有

$$(22)\quad \sum_{n\leq x}\Lambda(n)\left[\frac{x}{n}\right] = x\log x - x + O(\log x).$$

证明　在Enler求和公式（定理3.1）里取$f(t)=\log t$，我们得

$$\sum_{n\leq x}\log n = \int_1^x \log t\,dt + \int_1^x \frac{t-[t]}{t}dt - (x-[x])\log x$$

$$= x\log x - x + 1 + \int_1^x \frac{t-[t]}{t}dt + O(\log x).$$

因为

$$\int_1^x \frac{t-[t]}{t}\,dt = O\left(\int_1^x \frac{1}{t}dt\right) = O(\log x),$$

这就证明了(21)，并由(17)即得(22)． □

下面的定理是(22)的一个推论．

定理3.16　对$x\geq 2$，我们有

$$(23)\quad \sum_{p\leq x}\left[\frac{x}{p}\right]\log p = x\log x + O(x),$$

其中和式是对所有$\leq x$的素数展开．

证明　因为如果n不是一个素数的方幂，$\Lambda(n)=0$，所以我们有

$$\sum_{n\leqslant x}\left[\frac{x}{n}\right]\Lambda(n)=\sum_{p}\sum_{\substack{n=1\\p^m\leqslant x}}^{\infty}\left[\frac{x}{p^m}\right]\Lambda(p^m),$$

$p^m\leqslant x$得$p\leqslant x$，如果$p>x$，则$\left[\frac{x}{p^m}\right]=0$，所以我们能把最后的和式写为

$$\sum_{p\leqslant x}\sum_{m=1}^{\infty}\left[\frac{x}{p^m}\right]\log p=\sum_{p\leqslant x}\left[\frac{x}{p}\right]\log p+\sum_{p\leqslant x}\sum_{m=2}^{\infty}\left[\frac{x}{p^m}\right]\log p.$$

下面我们证明最后的和式为$O(x)$. 我们有

$$\begin{aligned}\sum_{p\leqslant x}\log p\sum_{m=2}^{\infty}\left[\frac{x}{p^m}\right]&\leqslant\sum_{p\leqslant x}\log p\sum_{m=2}^{\infty}\frac{x}{p^m}\\&=x\sum_{p\leqslant x}\log p\sum_{m=2}^{\infty}\left(\frac{1}{p}\right)^m\\&=x\sum_{p\leqslant x}\log p\cdot\frac{1}{p^2}\cdot\frac{1}{1-\frac{1}{p}}\\&=x\sum_{p\leqslant x}\frac{\log p}{p(p-1)}\\&\leqslant x\sum_{n=2}^{\infty}\frac{\log n}{n(n-1)}=O(x).\end{aligned}$$

于是我们证明了

$$\sum_{n\leqslant x}\left[\frac{x}{n}\right]\Lambda(n)=\sum_{p\leqslant x}\left[\frac{x}{p}\right]\log p+O(x),$$

再利用(22)就证明了(23). □

下一章我们将利用(23)去推导出发散级数$\sum\left(\frac{1}{p}\right)$的部分和的渐近公式.

3.12 Dirichlet乘积的部分和的另一个等式

我们利用定理3.10的更一般的说法来结束这一章．在第四章里将利用此定理去研究某些Dirichlet乘积的部分和．

在定理3.10里，我们写

$$F(x)=\sum_{n\leqslant x}f(n),\ G(x)=\sum_{n\leqslant x}g(n),$$

$$H(x)=\sum_{n\leqslant x}(f*g)(n),$$

于是

$$H(x)=\sum_{n\leqslant x}\sum_{d\mid n}f(d)g\left(\frac{n}{d}\right)=\sum_{\substack{q,d\\ qd\leqslant x}}f(d)g(q)$$

定理3.17　如果a与b是正实数，使得ab＝x，则有

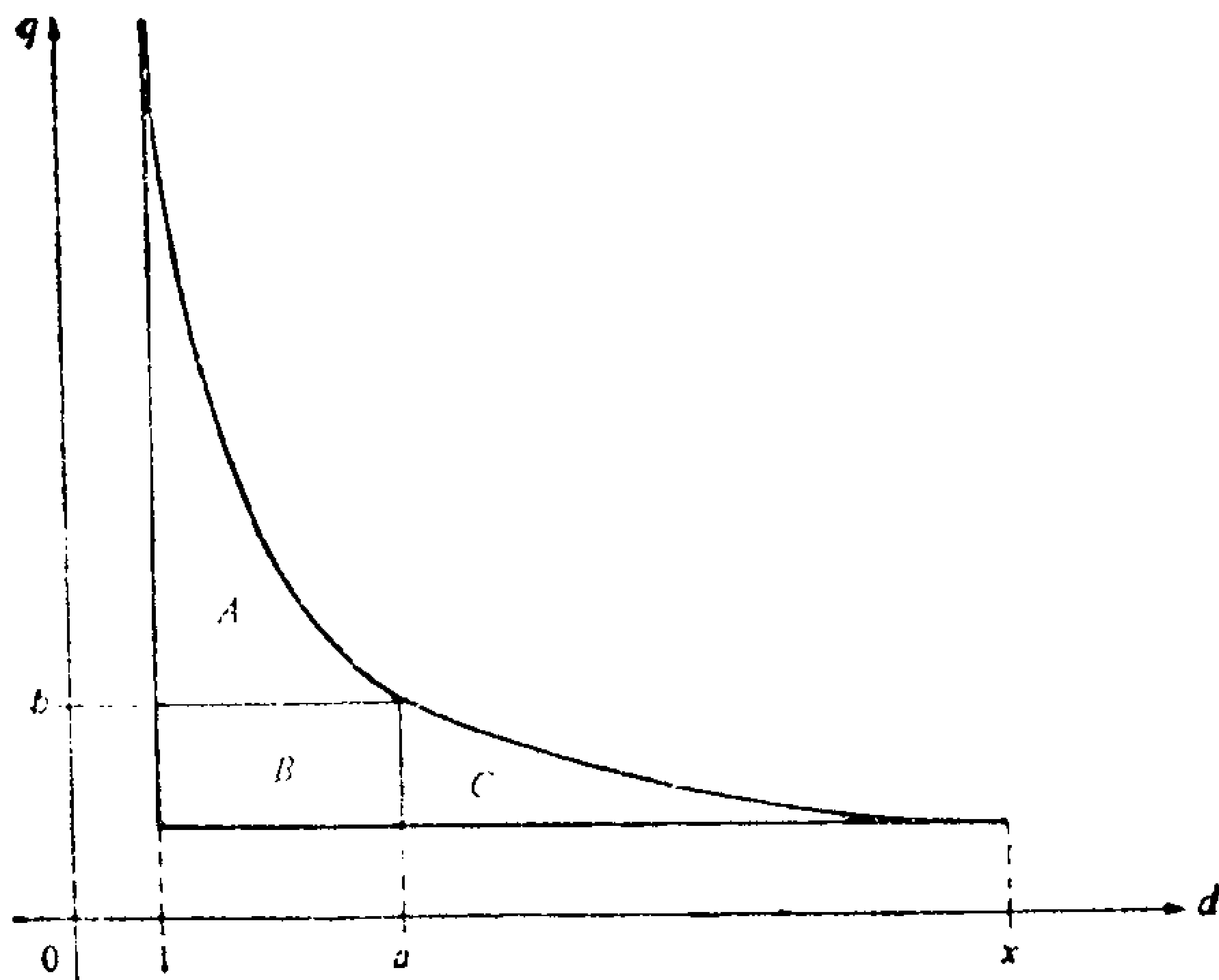
$$(24)\quad \sum_{\substack{q,d\\ qd\leqslant x}}f(d)g(q)=\sum_{n\leqslant a}f(n)G\left(\frac{x}{n}\right)+\sum_{n\leqslant b}g(n)F\left(\frac{x}{n}\right)-F(a)G(b).$$

证明　(24)式左端的和H(x)是在图3.4里表示的双曲线区域内的格点上展开的．我们把这个和分为两部分，一部分在A∪B的格点上展开，另一部分在B∪C的格点上展开．在B里的格点复盖了两次，所以我们有

$$H(x)=\sum_{d\leqslant a}\sum_{q\leqslant\frac{x}{d}}f(d)g(q)+\sum_{q\leqslant b}\sum_{d\leqslant\frac{x}{q}}f(d)g(q)-\sum_{d\leqslant a}\sum_{q\leqslant b}f(d)g(q),$$

此与(24)相同．□

注：分别取a＝1与b＝1，因为f(1)＝F(1)与g(1)＝G(1)，我们可得定理3.10里的两个等式．



（图3.4）

第三章习题

1．利用Euler求和公式，对$x\geqslant 2$，推导下列二式：

(a) $\displaystyle\sum_{n\leqslant x}\frac{\log n}{n}=\frac{1}{2}\log^2 x+A+O\left(\frac{\log x}{x}\right)$ A为常数．

(b) $\displaystyle\sum_{2\leqslant n\leqslant x}\frac{1}{n\log n}=\log(\log x)+B+O\left(\frac{1}{x\log x}\right)$

B为常数．

2．如果$x\geqslant 2$，证明

$\displaystyle\sum_{n\leqslant x}\frac{d(n)}{n}=\frac{1}{2}\log^2 x+2C\log x+O(1)$，其中C是Euler常数．

3．如果$x\geqslant 2$且$\alpha>0$，$\alpha\neq 1$，证明

$$\sum_{n\le x}\frac{d(n)}{n^{\alpha}}=\frac{x^{1-\alpha}\log x}{1-\alpha}+\zeta(\alpha)^{2}+O(x^{1-\alpha}).$$

4. 如果$x\geqslant2$，证明

(a) $$\sum_{n\le x}\frac{\mu(n)}{n}\left[\frac{x}{n}\right]^{2}=\frac{x^{2}}{\zeta(2)}+O(x\log x),$$

(b) $$\sum_{n\leqslant x}\frac{\mu(n)}{n}\left[\frac{x}{n}\right]=\frac{x}{\zeta(2)}+O(\log x).$$

5. 如果$x\geqslant1$，证明

(a) $$\sum_{n\le x}\varphi(n)=\frac{1}{2}\sum\mu(n)\left[\frac{x}{n}\right]^{2}+\frac{1}{2},$$

(b) $$\sum_{n\le x}\frac{\varphi(n)}{n}=\sum_{n\leqslant x}\frac{\mu(n)}{n}\left[\frac{x}{n}\right].$$

5题与4题的公式一起，说明对$x\geqslant2$，有

$$\sum_{n\le x}\varphi(n)=\frac{1}{2}\frac{x^{2}}{\zeta(2)}+O(x\log x),$$

$$\sum_{n\le x}\frac{\varphi(n)}{n}=\frac{x}{\zeta(2)}+O(\log x).$$

6. 如果$x\geqslant2$，证明

$$\sum_{n\le x}\frac{\varphi(n)}{n^{2}}=\frac{1}{\zeta(2)}\log x+\frac{C}{\zeta(2)}-A+O\left(\frac{\log x}{x}\right),$$

其中C是Euler常数而 $A=\sum_{n=1}^{x}\frac{\mu(n)\log n}{n^{2}}$.

7. 在下一章，我们将证明，如果$\alpha>1$，则有

$\sum_{n=1}^{\alpha}\frac{\mu(n)}{n}=\frac{1}{\zeta(2)}$. 假定这是成立的，证明

对$x\geqslant2$，$\alpha>1$，$\alpha\neq2$，我们有

$$\sum_{n\leq x}\frac{\varphi(n)}{n^{\alpha}}=\frac{x^{2-\alpha}}{2-\alpha}\frac{1}{\zeta(2)}+\frac{\zeta(\alpha-1)}{\zeta(\alpha)}$$
$$+O(x^{1-\alpha}\log x).$$

8. 如果$\alpha\leqslant1$而$x\geqslant2$，证明

$$\sum_{n\leq x}\frac{\varphi(n)}{n^{\alpha}}=\frac{x^{2-\alpha}}{2-\alpha}\frac{1}{\zeta(2)}+O(x^{1-\alpha}\log x).$$

9. 下一章我们将证明，在所有的素数上展开的无穷乘积$\Pi_p(1-p^{-2})$收敛于值$\frac{1}{\zeta(2)}=\frac{6}{\pi^2}$，先假定这是成立的，证明，

(a) $\frac{\sigma(n)}{n}<\frac{n}{\varphi(n)}<\frac{\pi^2}{6}\frac{\sigma(n)}{n}$，如果$n\geqslant2$.

[提示：利用公关$\varphi(n)=n\prod_{p\mid n}(1-p^{-1})$与关系式 $1+x+x^2+\cdots=\frac{1}{1-x}=\frac{1+x}{1-x^2}$还有$x=\frac{1}{p}$.]

(b) 如果$x\geqslant2$，证明

$$\sum_{n\leq x}\frac{n}{\varphi(n)}=O(x).$$

10. 如果$x\geqslant2$，证明

$$\sum_{n\leq x}\frac{1}{\varphi(n)}=O(\log x)$$

11. 令 $\varphi_1(n)=\frac{n\sum_{d\mid n}|\mu(d)|}{d}$，

(a) (c) 证明φ_1是积性的且$\varphi_1(n)=n\prod_{p\mid n}(1+p^{-1})$.

(b) 证明

$$\varphi_1(n)=\sum_{d^2\mid n}\mu(d)\sigma\left(\frac{n}{d^2}\right)$$

其中和是在满足$d^2\mid n$的那些n的约数d上展开.

(c) 证明

$$\sum_{n\leqslant x}\varphi_1(n)=\sum_{d\leqslant\sqrt{x}}\mu(d)S\left(\frac{x}{d^2}\right),$$ 其中

$S(x)=\sum_{k\leqslant x}\sigma(k)$，然后，利用定理3.4推证，

对$x\geqslant 2$，有

$$\sum_{n\leqslant x}\varphi_1(n)=\frac{\zeta(2)}{2\zeta(4)}x^2+O(x\log x).$$

同第7题一样，可以先假定$\sum_{n=1}^{\infty}\mu(n)n^{-\alpha}=\frac{1}{\zeta(2)}$

对$\alpha>1$是成立的.

12. 对实数$\alpha>0$与整数$k\geqslant 1$，确定下面的部分和

$$\sum_{\substack{n\leqslant x\\(n,k)=1}}\frac{1}{n^s}$$

的渐近公式. 并且当$x\to\infty$时，误差项趋于0. 对包含$s=1$的情形也是真实的.

最大整数函数的性质

对于每个实数x，符号$[x]$表示$\leqslant x$的最大整数. 13至16题描述最大整数函数的一些性质，其中x与y表示实数，n表示整数.

13. 证明下列各条的每一条：

(a) 如果$x=k+y$，这里k是整数，$0<y<1$，则$k=[x]$.

(b) $[x+n]=[x]+n$.

(c) $[-x]=\begin{cases}-[x] & \text{如果}x=[x],\\ -[x]-1 & \text{如果}x\neq[x].\end{cases}$

(d) $\left[\frac{x}{n}\right]=\left[\frac{[x]}{n}\right]$ 如果$n\geqslant 1$.

14．如$0<y<1$，问$[x]-[x-y]$的值可能是什么？

15．数$\{x\}=x-[x]$称为x的分数部分，它满足不等式$0\leqslant\{x\}<1$．当且仅当x是整数时，$\{x\}=0$．问$\{x\}+\{-x\}$的值能够是什么？

16．(a) 证明 $[2x]-2[x]$必为0或1．

(b) 证明 $[2x]+[2y]\geqslant[x]+[y]+[x+y]$．

17．证明 $[x]+\left[x+\frac{1}{2}\right]=[2x]$，更一般，

$$\sum_{k=0}^{n-1}\left[x+\frac{k}{n}\right]=[nx].$$

18．令$f(x)=x-[x]-\frac{1}{2}$，证明

$$\sum_{k=0}^{n-1}f\left(x+\frac{k}{n}\right)=f(nx),$$

并推导出

$$\left|\sum_{n=1}^{m}f\left(2^{n}x+\frac{1}{2}\right)\right|\leqslant 1$$

对所有$m\geqslant 1$与所有实数x．

19．给定正奇整数h与k，$(h,k)=1$，令$a=\frac{(k-1)}{2}$，$b=\frac{(h-1)}{2}$．

(a) 证明$\sum_{r=1}^{a}\left[\frac{hr}{k}\right]+\sum_{r=1}^{b}\left[\frac{kr}{h}\right]=ab$．［提示：格点．］

(b) 如果$(h,k)=d$．请给出一个相应的结果．

20．如果n是一个正整数，

证明$[\sqrt{n}+\sqrt{n+1}]=[\sqrt{4n+2}]$．

21．确定满足$[\sqrt{n}]$整除n的所有正整数n．

22．如果n是一个正整数，证明

$$\left[\frac{8n+13}{25}\right]-\left[\frac{n-12-\left[\frac{n-17}{25}\right]}{3}\right]$$

与n无关.

23. 证明

$$\sum_{n\leqslant x}\lambda(n)\left[\frac{x}{n}\right]=[\sqrt{x}].$$

24. 证明

$$\sum_{n\leqslant x}\left[\sqrt{\frac{x}{n}}\right]=\sum_{n\leqslant\sqrt{x}}\left[\frac{x}{n^2}\right].$$

25. 证明

$$\sum_{k=1}^{n}\left[\frac{k}{2}\right]=\left[\frac{n^2}{4}\right]$$

与

$$\sum_{k=1}^{n}\left[\frac{k}{3}\right]=\left[\frac{n(n-1)}{6}\right].$$

26. 如果a＝1，2，…，7. 证明存在一个整数b（与a有关）使得

$$\sum_{k=1}^{n}\left[\frac{k}{a}\right]=\left[\frac{(2n+b)^2}{8a}\right].$$

第四章　素数分布的几个基本定理

4.1　引言

如果$x>0$，令$\pi(x)$表示不超过x的素数的个数．由于有无穷多个素数，于是随$x\to\infty$而$\pi(x)\to\infty$．从18世纪以来，x的函数$\pi(x)$的变化情况一直是许多著名的数学家认真研究的对象．由素数表的检验提示，Gauss(1792年)与Legendve(1798年)猜想$\pi(x)$趋于$\frac{x}{\log x}$，即

$$\lim_{x\to\infty}\frac{\pi(x)\log x}{x}=1.$$

这个猜想在1896年由Hadamard[28]与de la Vallee Poussin[71]首先证明并且这个猜想现在就是著名的素数定理．

素数定理的证明按它们所使用的方法通常分为解析的与初等的．Hadamard与de la Vallee Poussin的证明是解析的，该证明利用了复变函数的理论与Riemann zeta函数的性质．初等的证明在1949年由A．Selberg与P．Erdös所发现，他们的证明完全不用zeta函数也不利用复变函数的理论但却是十分复杂的．本章末尾我们给出这个初等证明的主要特征的简短要点．在第13章里我们介绍一下简短的解析证明，

它比初等证明更明白些.

本章涉及素数方面的几个初始而且基本的定理，特别，我们将证明，素数定理能表为几个等价的形式.

例如，我们将证明，素数定理等价于渐近公式

(1) $\sum_{n\leq x}\Lambda(n)\sim x$ 当$x\to\infty$时.

Mangoldt函数$\Lambda(n)$的部分和定义一个函数，这是由Chebyshev在1848年提出来的.

4.2 Chebyshev函数$\psi(x)$与$\vartheta(x)$

定义 对$x>1$，我们用公式

$$\psi(x)=\sum_{n\leq x}\Lambda(n)$$

定义Chebyshev ψ—函数. 从而(1)式里的渐近公式为

(2) $\lim_{x\to\infty}\frac{\psi(x)}{x}=1$.

因为，如果n不是一个素数的方幂，则有$\Lambda(n)=0$. 于是我们能够写出$\psi(x)$的定义如下：

$$\psi(x)=\sum_{n\leq x}\Lambda(n)=\sum_{m=1}^{\infty}\sum_{\substack{p\\p^m\leq x}}\Lambda(p^m)$$

$$=\sum_{m=1}^{\infty}\sum_{p\leq x^{\frac{1}{m}}}\log p.$$

m上的这个和实际上是一个有限和. 事实上，如果$x^{\frac{1}{m}}<2$，即如果$\left(\frac{1}{m}\right)\log x<\log 2$，或者如果

$$m>\frac{\log x}{\log 2}=\log_2 x,$$

p上的和是空的．因此我们有

$$\psi(x)=\sum_{m\leqslant\log_2 x}\sum_{p\leqslant x^{\frac{1}{m}}}\log p.$$

这就能以微小形式的差异写出另一个Chebyshev函数．

定义　如果$x>0$，我们用等式

$$g(x)=\sum_{p\leqslant x}\log p$$

定义Chebyshev g—函数．其中p通过所有$\leqslant x$的素数．

$\psi(x)$的最后一个式子可以重新写为

$$(3)\quad \psi(x)=\sum_{m\leqslant\log_2 x}g(x^{\frac{1}{m}}).$$

下面的定理与两个商$\frac{\psi(x)}{x}$和$\frac{g(x)}{x}$有关．

定理4.1　对$x>0$，我们有

$$0\leqslant\frac{\psi(x)}{x}-\frac{g(x)}{x}\leqslant\frac{(\log x)^2}{2\sqrt{x}\log 2}.$$

注:这个不等式意即

$$\lim_{x\to\infty}\left(\frac{\psi(x)}{x}-\frac{g(x)}{x}\right)=0.$$

换言之，如果$\frac{\psi(x)}{x}$与$\frac{g(x)}{x}$之一趋于一个极限，那么另一个也趋于一个极限并且这两个极限相等．

证明　由(3)我们得出

$$0\leqslant\psi(x)-g(x)=\sum_{2\leqslant m\leqslant\log_2 x}g(x^{\frac{1}{m}}),$$

但由$g(x)$的定义我们有不等式

$$g(x)\leqslant\sum_{p\leqslant x}\log x\leqslant x\log x,$$

所以

$$0 \leqslant \psi(x) - g(x) \leqslant \sum_{2 \leqslant m \leqslant \log \frac{x}{2}} x^{\frac{1}{m}} \log(x^{\frac{1}{m}})$$

$$\leqslant (\log_2 x)\sqrt{x} \log\sqrt{x} = \frac{\log x}{\log 2} \cdot \frac{\sqrt{x}}{2} \log x$$

$$= \frac{\sqrt{x}(\log x)^2}{2\log 2}.$$

用x去除，即得定理. □

4.3 联系g(x)与π(x)的关系式

本节，我们将得到g(x)与π(x)的两个关系式，它们将被用于证明素数定理等价于极限式

$$\lim_{x \to \infty} \frac{g(x)}{x} = 1.$$

π(x)与g(x)两个函数都是阶梯函数并在素数上跳跃．π(x)在每一个素数p上有一个跳跃．而g(x)在p上有一个logp的跳跃．含有这类阶梯函数的和能表为下面定理的平均值的积分．

定理4.2　Abel等式．对任一数论函数a(n)，令

$$A(x) = \sum_{n \leqslant x} a(n),$$

其中，A(x)＝0当x＜1时．假设f在区间[y，x]上有连续导数，其中0＜y＜x，那么我们有

$$(4) \quad \sum_{y < n \leqslant x} a(n)f(n) = A(x)f(x) - A(y)f(y) - \int_y^x A(t)f'(t)dt.$$

证明　令k＝[x]与m＝[y]，于是A(x)＝A(k)并且A(y)＝A(m)，则有

$$\sum_{y<n\leqslant x} a(n)f(n)$$

$$= \sum_{n=m+1}^{k} a(n)f(n) = \sum_{n=m+1}^{k} \{A(n)-A(n-1)\} f(n)$$

$$= \sum_{n=m+1}^{k} A(n)f(n) - \sum_{n=m}^{k-1} A(n)f(n+1)$$

$$= \sum_{n=m+1}^{k-1} A(n)\{f(n)-f(n+1)\}$$

$$+ A(k)f(k) - A(m)f(m+1)$$

$$= -\sum_{n=m+1}^{k-1} A(n)\int_{n}^{n+1} f'(t)dt$$

$$+ A(k)f(k) - A(m)f(m+1)$$

$$= -\sum_{n=m+1}^{k-1}\int_{n}^{n+1} A(t)f'(t)dt$$

$$+ A(k)f(k) - A(m)f(m+1)$$

$$= -\int_{m+1}^{k} A(t)f'(t)dt + A(x)f(x) - \int_{k}^{x} A(t)f'(t)dt$$

$$- A(y)f(y) - \int_{y}^{m+1} A(t)f'(t)dt$$

$$= A(x)f(x) - A(y)f(y) - \int_{y}^{x} A(t)f'(t)dt. \qquad \square$$

替代的证明．对于熟悉Riemann-Stieltjes积分（参阅[2]，第7章）的读者可以得到（4）的一个简短的证明．因为$A(x)$是一个阶梯函数而$f(n)$在每一个整数n上跳跃，所以（4）式的和能表示为Riemann-Stieltjes积分，

$$\sum_{y<n\leqslant x} a(n)f(n) = \int_{y}^{x} f(t)dA(t).$$

由分部积分得

$$\sum_{y<n\leqslant x} a(n)f(n) = f(x)A(x) - f(y)A(y)$$

$$-\int_y^x A(t)df(t)$$

$$=f(x)A(x)-f(y)A(y)$$

$$-\int_y^x A(t)f'(t)dt. \qquad \square$$

注：因为当$t<1$时，$A(t)=0$，所以当$y<1$时，(4)式有形式

$$(5)\quad \sum_{n\leqslant x} a(n)f(n)=A(x)f(x)-\int_1^x A(t)f'(t)dt.$$

由(4)式也容易推出著名的Euler求和公式．实际上，如果对所有的$n\geqslant 1$，$a(n)=1$，我们得出$A(x)=[x]$且(4)式推出

$$\sum_{y<n\leqslant x} f(n)=f(x)[x]-f(y)[y]-\int_y^x [t]f'(t)dt,$$

由此与分部积分公式

$$\int_y^x tf'(t)dt=xf(x)-yf(y)-\int_y^x f(t)dt,$$

我们即可得到Euler求和公式．（定理3.1）

现在我们利用(4)式并以积分来表示$g(x)$与$\pi(x)$.

定理4.3　对$x\geqslant 2$，我们有

$$(6)\quad g(x)=\pi(x)\log x-\int_2^x \frac{\pi(t)}{t}dt$$

与

$$(7)\quad \pi(x)=\frac{g(x)}{\log x}+\int_2^x \frac{g(t)}{t\log^2 t}dt.$$

证明　令$a(n)$表示素数的特征函数，即

$$a(n)=\begin{cases}1 & \text{若}n\text{是素数},\\ 0 & \text{其它}.\end{cases}$$

则有

$$\pi(x)=\sum_{p\leqslant x}1=\sum_{1<n\leqslant x}a(n),\quad g(x)=\sum_{p\leqslant x}\log p$$
$$=\sum_{1<n\leqslant x}a(n)\log n.$$

在(4)里取$f(x)=\log x$与$y=1$，我们得

$$g(x)=\sum_{1<n\leqslant x}a(n)\log n$$
$$=\pi(x)\log x-\pi(1)\log 1-\int_1^x\frac{\pi(t)}{t}dt,$$

因为，对$t<2$，$\pi(t)=0$，它就证明了(6)．

其次，令$b(n)=a(n)\log n$并写

$$\pi(x)=\sum_{\frac{3}{2}<n\leqslant x}b(n)\frac{1}{\log n},\quad g(x)=\sum_{n\leqslant x}b(n),$$

在(4)式里取$f(x)=\frac{1}{\log x}$与$y=\frac{3}{2}$，得

$$\pi(x)=\frac{g(x)}{\log x}-\frac{g(\frac{3}{2})}{\log\frac{3}{2}}+\int_{\frac{3}{2}}^x\frac{g(t)}{t\log^2 t}dt,$$

因为当$t<2$时，$g(t)=0$，这就证明了(7)式．□

4.4 素数定理的几个等价形式

定理4.4 下面几个式子是逻辑等价的：

(8) $\lim\limits_{x\to\infty}\frac{\pi(x)\log x}{x}=1.$

(9) $\lim\limits_{x\to\infty}\frac{g(x)}{x}=1.$

(10) $\lim\limits_{x\to\infty}\frac{\psi(x)}{x}=1.$

证明　分别由(6)与(7)得

$$\frac{g(x)}{x}=\frac{\pi(x)\log x}{x}-\frac{1}{x}\int_2^x\frac{\pi(t)}{t}dt$$

与

$$\frac{\pi(x)\log x}{x}=\frac{g(x)}{x}+\frac{\log x}{x}\int_2^x\frac{g(t)dt}{t\log^2 t}.$$

为证明由(8)推出(9)，我们只需证明(8)推出

$$\lim_{x\to\infty}\frac{1}{x}\int_2^x\frac{\pi(t)}{t}dt=0.$$

但(8)即$\frac{\pi(t)}{t}=0\left(\frac{1}{\log t}\right)$对$t\geqslant 2$，所以

$$\frac{1}{x}\int_2^x\frac{\pi(t)}{t}dt=0\left(\frac{1}{x}\int_2^x\frac{dt}{\log t}\right),$$

而

$$\int_2^x\frac{dt}{\log t}=\int_2^{\sqrt{x}}\frac{dt}{\log t}+\int_{\sqrt{x}}^x\frac{dt}{\log t}$$

$$\leqslant\frac{\sqrt{x}}{\log 2}+\frac{x-\sqrt{x}}{\log\sqrt{x}},$$

所以

$$\frac{1}{x}\int_2^x\frac{dt}{\log t}\to 0\quad 当x\to\infty时.$$

这证明了由(8)推出(9).

为证明由(9)推出(8)，我们只需证(9)推出

$$\lim_{x\to\infty}\frac{\log x}{x}\int_2^x\frac{g(t)dt}{t\log^2 t}=0.$$

但(9)即$g(t)=0(t)$，所以

$$\frac{\log x}{x}\int_2^x\frac{g(t)dt}{t\log^2 t}=0\left(\frac{\log x}{x}\int_2^x\frac{dt}{\log^2 t}\right).$$

而

$$\int_2^x \frac{dt}{\log^2 t} = \int_2^{\sqrt{x}} \frac{dt}{\log^2 t} + \int_{\sqrt{x}}^x \frac{dt}{\log^2 t}$$

$$\leqslant \frac{\sqrt{x}}{\log^2 2} + \frac{x-\sqrt{x}}{\log^2 \sqrt{x}},$$

于是

$$\frac{\log x}{x}\int_2^x \frac{dt}{\log^2 t} \to 0 \quad 当x\to\infty时,$$

这证明了(8)推出(9)，所以(8)与(9)是等价的.

由定理4.1已经知道(9)与(10)是等价的. □

下面的定理把素数定理与第n个素数的渐近值联系起来.

定理4.5　令p_n是第n个素数，则下面几个渐近式是逻辑等价的：

(11) $\lim\limits_{x\to\infty} \frac{\pi(x)\log x}{x} = 1$

(12) $\lim\limits_{x\to\infty} \frac{\pi(x)\log\pi(x)}{x} = 1$

(13) $\lim\limits_{x\to\infty} \frac{P_n}{n\log n} = 1$

证明　我们证明，(11)推出(12)，(12)推出(13)，(13)推出(12)，(12)推出(11).

假设(11)式成立，两边取对数，得

$$\lim_{x\to\infty}[\log\pi(x) + \log\log x - \log x] = 0.$$

或者

$$\lim_{x\to\infty}\left[\log x\left(\frac{\log\pi(x)}{\log x} + \frac{\log\log x}{\log x} - 1\right)\right] = 0,$$

因为当$x\to\infty$时，$\log x\to\infty$，由此得

$$\lim_{x\to\infty}\left(\frac{\log\pi(x)}{\log x}+\frac{\log\log x}{\log x}-1\right)=0.$$

我们得

$$\lim_{x\to\infty}\frac{\log\pi(x)}{\log x}=1.$$

此式与(11)一起，得出(12)式.

现在设(12)式成立. 如果$x=P_n$，则$\pi(x)=n$且

$$\pi(x)\log\pi(x)=n\log n,$$

所以(12)式推出

$$\lim_{n\to\infty}\frac{n\log n}{p_n}=1.$$

这样，由(12)推出了(13).

下面设(13)成立. 给定x，由不等式$p_n\leqslant x<p_{n+1}$确定n，所以$n=\pi(x)$，用$n\log n$去除，得

$$\frac{p_n}{n\log n}\leqslant\frac{x}{n\log n}<\frac{p_{n+1}}{n\log n}$$

$$=\frac{p_{n+1}}{(n+1)\log(n+1)}\cdot\frac{(n+1)\log(n+1)}{n\log n}.$$

令$n\to\infty$并利用(13)，得

$$\lim_{n\to\infty}\frac{x}{n\log n}=1\text{或}\lim_{x\to\infty}\frac{x}{\pi(x)\log\pi(x)}=1.$$

因此，(13)推出(12).

最后，我们证明(12)推出(11)，(12)取对数，得

$$\lim_{x\to\infty}(\log\pi(x)+\log\log\pi(x)-\log x)=0,$$

或者

$$\lim_{x\to\infty}\left[\log\pi(x)\left(1+\frac{\log\log\pi(x)}{\log\pi(x)}-\frac{\log x}{\log\pi(x)}\right)\right]$$

$$=0.$$

因为$\log\pi(x)\to\infty$，立即得出

$$\lim_{x\to\infty}\left(1+\frac{\log\log\pi(x)}{\log\pi(x)}-\frac{\log x}{\log\pi(x)}\right)=0,$$

或者

$$\lim_{x\to\infty}\frac{\log x}{\log\pi(x)}=1.$$

此与(12)一起得出(11).

4.5　$\pi(n)$与p_n的一些不等式

素数定理说明，当$x\to\infty$时，$\pi(n)\sim n/\log n$. 下面的定理说明，$n/\log n$是$\pi(n)$的确切的阶. 虽然经过极大的努力后可以得到较好的不等式（参阅〔60〕），由于证明的初等，下面的定理仍是有兴趣的.

定理4.6　对每一个整数$n>2$，我们有

(14) $$\frac{1}{6}\frac{n}{\log n}<\pi(n)<6\frac{n}{\log n}.$$

证明　我们从不等式

(15) $$2^n\leqslant\binom{2n}{n}<4^n$$

开始，其中$\binom{2n}{n}=\frac{(2n)!}{n!n!}$是二项式系数，(15)右边的不等式是由下面的关系式得到的，

$$4^n=(1+1)^{2n}=\sum_{k=0}^{2n}\binom{2n}{k}>\binom{2n}{n}.$$

左边的不等式用归纳法容易证明. 将(15)式取对数，得

(16) $$n\log 2\leqslant\log(2n)!-2\log n!<n\log 4.$$

但定理3.14指出

$$\log n! = \sum_{p \leqslant n} \alpha(p) \log p,$$

其中和式对素数展开而$\alpha(p)$由

$$\alpha(p) = \sum_{m=1}^{\left[\frac{\log n}{\log p}\right]} \left[\frac{n}{p^m}\right]$$

给定．于是有

$$(17)\quad \log(2n)! - 2\log n! = \sum_{p \leqslant 2n} \sum_{m=1}^{\left[\frac{\log 2n}{\log p}\right]} \left\{\left[\frac{2n}{p^m}\right] - 2\left[\frac{n}{p^m}\right]\right\} \log p.$$

因为$[2x]-2[x]$为0或1，所以由(16)左边的不等式得出

$$n\log 2 \leqslant \sum_{p \leqslant 2n} \left(\sum_{m=1}^{\left[\frac{\log 2n}{\log p}\right]} 1\right) \log p \leqslant \sum_{p \leqslant 2n} \log 2n$$
$$= \pi(2n) \log 2n.$$

这给我们

$$(18)\quad \pi(2n) \geqslant \frac{n\log 2}{\log 2n} = \frac{2n}{\log 2n} \frac{\log 2}{2} > \frac{1}{4} \frac{2n}{\log 2n},$$

这因为$\log 2 > \frac{1}{2}$．对于奇数整数我们有

$$\pi(2n+1) \geqslant \pi(2n) > \frac{1}{4} \frac{2n}{\log 2n}$$

$$> \frac{1}{4} \frac{2n}{2n+1} \frac{2n+1}{\log(2n+1)}$$

$$\geqslant \frac{1}{6} \frac{2n+1}{\log(2n+1)},$$

这因为$\frac{2n}{(2n+1)} \geqslant \frac{2}{3}$．此式与(18)式一起给我们

$$\pi(n) > \frac{1}{6}\ \frac{n}{\log n}$$

对所有$n \geqslant 2$成立．它证明了(14)左边的不等式．

为了证明另一个不等式，我们回到(17)式，取出对应于$m=1$那一项，余下的项都是非负的，所以有

$$\log(2n)! - 2\log n! \geqslant \sum_{p \leqslant 2n} \left\{ \left[\frac{2n}{p}\right] - 2\left[\frac{n}{p}\right] \right\} \log p.$$

对于在区间$n < p \leqslant 2n$中的那些素数p，我们有

$$\left[\frac{2n}{p}\right] - 2\left[\frac{n}{p}\right] = 1, \text{所以}$$

$$\log(2n)! - 2\log n! \geqslant \sum_{n < p \leqslant 2n} \log p = g(2n) - g(n).$$

于是(16)推出$g(2n) - g(n) < n\log 4$.

特别，当n是2的一个方幂时，这给出

$$g(2^{r+1}) - g(2^r) < 2^r \log 4 = 2^{r+1} \log 2.$$

在$r=0, 1, 2, \cdots, K$上求和，左边各项加在一起，我们得

$$g(2^{k+1}) < 2^{k+2} \log 2.$$

现在我们选取这样的K，使$2^k \leqslant n < 2^{k+1}$，得

$$g(n) \leqslant g(2^{k+1}) < 2^{k+2} \log 2 \leqslant 4n \log 2.$$

但当$0 < \alpha < 1$时我们有

$$(\pi(n) - \pi(n^\alpha)) \log n^\alpha < \sum_{n^\alpha < p \leqslant n} \log p \leqslant g(n) < 4n \log 2.$$

于是

$$\pi(n) < \frac{4n\log 2}{\alpha \log n} + \pi(n^\alpha) < \frac{4n\log 2}{\alpha \log n} + n^\alpha$$

$$=\frac{n}{\log n}\left(\frac{4\log 2}{\alpha}+\frac{\log n}{n^{1-\alpha}}\right).$$

如果$c>0$且$x\geqslant 1$，则函数$f(x)=x^{-c}\log x$在$x=e^{\frac{1}{c}}$处达到最大值．所以$n^{-c}\log n\leqslant\frac{1}{(ce)}$将$n\geqslant 1$成立．在$\pi(n)$的最后的不等式里取$\alpha=\frac{2}{3}$，得

$$\pi(n)<\frac{n}{\log n}\left(6\log 2+\frac{3}{e}\right)<6\frac{n}{\log n}.$$

证明完成．

利用定理4.6能够得到第n个素数大小的上下界．

定理4.7　对$n\geqslant 1$，第n个素数P_n满足不等式

(19) $\frac{1}{6}n\log n<P_n<12\left(n\log n+n\log\frac{12}{e}\right).$

证明　如果$K=p_K$，那么$K\geqslant 2$且$n=\pi(K)$，由(14)我们有

$$n=\pi(K)<6\frac{K}{\log K}=6\frac{p_n}{\log p_n},$$

于是

$$P_n>\frac{1}{6}n\log p_n>\frac{1}{6}n\log n,$$

这给出了(19)的下界．

为得到上界，我们再利用(14)，写

$$n=\pi(K)>\frac{1}{6}\frac{K}{\log K}=\frac{1}{6}\frac{p_n}{\log p_n},$$

由此得

(20) $p_n<6n\log p_n$.

因为$\log x\leqslant\left(\frac{2}{e}\right)\sqrt{x}$，所以，当$x\geqslant 1$时，我们有$\log p_n\leqslant$

$\left(\frac{2}{e}\right)\sqrt{P_n}$，所以(20)推出

$$\sqrt{p_n}<\frac{12}{e}n.$$

因此

$$\frac{1}{2}\log p_n<\log n+\log\frac{12}{e}.$$

由此并利用(20)，我们得

$$p_n<6n\left(2\log n+2\log\frac{12}{e}\right).$$

这就证明了(19)式中的上界. □

注：(19)式的上界再一次说明级数 $\sum_{n=1}^{\infty}p_n^{-1}$ 发散，用它与 $\sum_{n=2}^{\infty}(n\log n)^{-1}$ 比较而得.

4.6 Shapiro Tauberian定理

我们曾经指出，素数定理等价于渐近式

$$(21)\quad \frac{1}{x}\sum_{n\leqslant x}\Lambda(n)\sim 1 \qquad 当x\to\infty时.$$

在定理3.15里我们推出过一个有关的渐近式

$$(22)\quad \sum_{n\leqslant x}\Lambda(n)\left[\frac{x}{n}\right]=x\log x-x+O(\log x).$$

(21)与(22)里的两个和都是函数$\Lambda(n)$的加权平均值. (21)里的每一项是$\Lambda(n)$乘以加权函数$\frac{1}{x}$，而(22)里是乘以$\left[\frac{x}{n}\right]$.

关于同一函数的不同加权平均值的定理称为Tauberian定理，下面我们讨论的Tauberian定理是由Shapiro[64]在

1950年证明的，它把形如$\sum_{n\leqslant x}a(n)$的和与形如$\sum_{n\leqslant x}a(n)\left[\frac{x}{n}\right]$的和联系起来，其中a(n)是非负的.

定理4.8　令$\{a(n)\}$是一个非负序列，使得

$$(23)\quad \sum_{n\leqslant x}a(n)\left[\frac{x}{n}\right]=x\log x+O(x)\ \text{对所有}x\geqslant 1.$$

那么：

(a) 对$x\geqslant 1$，我们有

$$\sum_{n\leqslant x}\frac{a(n)}{n}=\log x+O(1).$$

（换言之，在(23)里去掉方括号推导出一个正确的结果.）

(b) 存在一个常数$B>0$，使得

$$\sum_{n\leqslant x}a(n)\leqslant Bx\quad \text{对所有的}x\geqslant 1.$$

(c) 存在一个常数$A>0$与$x_0>0$　使得

$$\sum_{n\leqslant x}a(n)\geqslant Ax\quad \text{对所有}x\geqslant x_0.$$

证明　令$S(x)=\sum_{n\leqslant x}a(n)$，$T(x)=\sum_{n\leqslant x}a(n)\left[\frac{x}{n}\right]$.

我们先证明(b). 为此建立不等式

$$(24)\quad S(x)-S\left(\frac{x}{2}\right)\leqslant T(x)-2T\left(\frac{x}{2}\right).$$

我们写

$$T(x)-2T\left(\frac{x}{2}\right)=\sum_{n\leqslant x}\left[\frac{x}{n}\right]a(n)-2\sum_{n\leqslant\frac{x}{2}}\left[\frac{x}{2n}\right]a(n)$$

$$=\sum_{n\leqslant\frac{x}{2}}\left(\left[\frac{x}{n}\right]-2\left[\frac{x}{2n}\right]\right)a(n)$$

$$+\sum_{\frac{x}{2}<n\leqslant x}\left[\frac{x}{n}\right]a(n).$$

因为$[2y]-2[y]$为0或1，第一个和式是非负的，所以有

$$T(x)-2T\left(\frac{x}{2}\right)\geqslant\sum_{\frac{x}{2}<n\leqslant x}\left[\frac{x}{n}\right]a(n)$$

$$=\sum_{\frac{x}{2}<n\leqslant x}a(n)=S(x)-S\left(\frac{x}{2}\right).$$

这证明了(24)．但(23)推出

$$T(x)-2T\left(\frac{x}{2}\right)=x\log x+O(x)$$

$$-2\left(\frac{x}{2}\log\frac{x}{2}+O(x)\right)=O(x),$$

于是(24)推出$S(x)-S\left(\frac{x}{2}\right)=O(x)$，这就是说，存在某个常数K，使得

$$S(x)-S\left(\frac{x}{2}\right)\leqslant Kx\quad 对所有x\geqslant 1.$$

逐次用$\frac{x}{2}$，$\frac{x}{4}$，…去代替x，得

$$S\left(\frac{x}{2}\right)-S\left(\frac{x}{4}\right)\leqslant K\frac{x}{2},$$

$$S\left(\frac{x}{4}\right)-S\left(\frac{x}{8}\right)\leqslant K\frac{x}{4},$$

等等．注意，当$2^n>x$时，$S\left(\frac{x}{2^n}\right)=0$，把这些不等式加起来，得

$$S(x)\leqslant Kx\left(1+\frac{1}{2}+\frac{1}{4}+\cdots\right)=2Kx.$$

取$B=2K$就证明了(b)．

下面我们证明(a). 我们写$\left[\frac{x}{n}\right]=\left(\frac{x}{n}\right)+O(1)$，得

$$T(x)=\sum_{n\leq x}\left[\frac{x}{n}\right]a(n)=\sum_{n\leq x}\left(\frac{x}{n}+O(1)\right)a(n)$$

$$=x\sum_{n\leq x}\frac{a(n)}{n}+O\left(\sum_{n\leq x}a(n)\right)$$

$$=x\sum_{n\leq x}\frac{a(n)}{n}+O(x),$$

根据(b). 于是

$$\sum_{n\leq x}\frac{a(n)}{n}=\frac{1}{x}T(x)+O(1)=\log x+O(1).$$

这证明了(a).

最后，我们证明(c). 令

$$A(x)=\sum_{n\leq x}\frac{a(n)}{n}.$$

则(a)可写为：

$$A(x)=\log x+R(x),$$

其中$R(x)$是误差项. 因为$R(x)=O(1)$，所有对某个$M>0$，有$|R(x)|\leq M$.

选择α满足$0<\alpha<1$，（我们立即会更精确地确定α），并讨论差

$$A(x)-A(\alpha x)=\sum_{\alpha x<n\leq x}\frac{a(n)}{n}$$

$$=\sum_{n\leq x}\frac{a(n)}{n}-\sum_{n\leq\alpha x}\frac{a(n)}{n}.$$

当$x\geq1$且$\alpha x\geq1$时，我们可利用$A(x)$的渐近公式写

$$A(x)-A(\alpha x)=\log x+R(x)-(\log\alpha x+R(\alpha x))$$

$$=-\log\alpha+R(x)-R(\alpha x)$$

$$\geqslant -\log\alpha - |R(x)| - |R(\alpha x)|$$
$$\geqslant -\log\alpha - 2M.$$

现在选择α使$-\log\alpha - 2M = 1$，这要求$\log\alpha = -2M-1$，$\alpha = e^{-2M-1}$. 注意$0<\alpha<1$. 对此α，我们有不等式

$$A(x) - A(\alpha x) \geqslant 1 \quad 当 x \geqslant \frac{1}{2} 时.$$

但是

$$A(x) - A(\alpha x) = \sum_{\alpha x < n \leqslant x} \frac{a(n)}{n} \leqslant \frac{1}{\alpha x} \sum_{n \leqslant x} a(n)$$
$$= \frac{S(x)}{\alpha x},$$

于是

$$\frac{S(x)}{\alpha x} \geqslant 1 \quad 当 x \geqslant \frac{1}{\alpha} 时.$$

因此，当$x \geqslant \frac{1}{\alpha}$时，$S(x) \geqslant \alpha x$，取$A = \alpha$与$x_0 = \frac{1}{\alpha}$就 证 明了(c).

4.7 Shapiro定理的应用

等式(22)推出

$$\sum_{n \leqslant x} \Lambda(n) \left[\frac{x}{n}\right] = n\log x + O(x),$$

因为$\Lambda(n) \geqslant 0$，我们能够利用Shapiro定理以及$a(n) = \Lambda(n)$去得到：

定理4.9 对所有$x \geqslant 1$，我们有

$$(25) \quad \sum_{n \leqslant x} \frac{\Lambda(n)}{n} = \log x + O(1).$$

还有，存在正的常数C_1与C_2使得

$$\psi(x)\leqslant C_1x \quad 对所有x\geqslant 1$$

且

$$\psi(x)\geqslant C_2x \quad 对所有充分大的x.$$

另一个应用能由定理3.16已证过的渐近公式

$$\sum_{p\leqslant x}\left[\frac{x}{p}\right]\log p=x\log x+O(x)$$

导出，它能写为

$$(26)\quad \sum_{n\leqslant x}\Lambda_1(n)\left[\frac{x}{n}\right]=x\log x+O(x),$$

其中Λ_1是如下定义的函数：

$$\Lambda_1(n)=\begin{cases}\log p & 当n是一个素数时,\\ 0 & 其它.\end{cases}$$

因为$\Lambda_1(n)\geqslant 0$，等式(26)说明Shapiro定理的前提条件在$a(x)=\Lambda_1(n)$时是满足的．因为$g(x)=\sum_{n\leqslant x}\Lambda_1(n)$，由Shapiro定理的(a)能给出下面的渐近公式．

定理4.10　对所有$x\geqslant 1$，我们有

$$(27)\quad \sum_{p\leqslant x}\frac{\log p}{p}=\log x+O(1).$$

还存在正的常数c_1与c_2使得

$$g(x)\leqslant c_1x \quad \text{对所有}x\geqslant 1,$$

$$g(x)\geqslant c_2x \quad \text{对所有充分大的}x.$$

在定理3.11里我们证明过

$$\sum_{n\leqslant x}f(n)\left[\frac{x}{n}\right]=\sum_{n\leqslant x}F\left(\frac{x}{n}\right)$$

对任一数论函数$f(n)$以及部分和$F(x)=\sum_{n\leqslant x}f(n)$成立．因为$\psi(x)=\sum_{n\leqslant x}\Lambda(n)$，$g(x)=\sum_{n\leqslant x}\Lambda_1(n)$，所以(22)式与(26)式

的渐近公式能直接用$\psi(x)$与$g(x)$来表示，我们 把 它表为定理形式.

定理4.11 对所有$x\geqslant 1$，我们有

$$(28)\quad \sum_{x\leqslant n}\psi\left(\frac{x}{n}\right)=x\log x-x+O(\log x)$$

与

$$\sum_{n\leqslant x}g\left(\frac{x}{n}\right)=x\log x+O(x).$$

4.8 部分和$\sum_{p\leqslant x}\left(\frac{1}{p}\right)$的一个渐近公式

在第一章里我们证明过级数$\sum\left(\frac{1}{p}\right)$发散. 现 在 我们得到它的部分和的一个渐近公式. 这个结果是定理4.10里等式(27)的一个应用.

定理4.12 存在一个常数A，使得

$$(29)\quad \sum_{p\leqslant x}\frac{1}{p}=\log\log x+A+O\left(\frac{1}{\log x}\right)\text{对所有}x\geqslant 2.$$

证明 令

$$A(x)=\sum_{p\leqslant x}\frac{\log p}{p}$$

并令

$$a(n)=\begin{cases}1 & \text{若}n\text{是素数,}\\ 0 & \text{其它.}\end{cases}$$

则有

$$\sum_{p\leqslant x}\frac{1}{p}=\sum_{n\leqslant x}\frac{a(n)}{n},\quad A(x)=\sum_{n\leqslant x}\frac{a(n)}{n}\log n.$$

因此，当我们在定 理4.2里取$f(t)=\frac{1}{\log t}$时，由于对$t<2$，

$A(t)=0$，所以我们有

$$(30)\quad \sum_{p\leq x}\frac{1}{p}=\frac{A(x)}{\log x}+\int_2^x\frac{A(t)}{t\log^2 t}dt.$$

由(27)式我们有$A(x)=\log x+R(x)$，这里$R(x)=O(1)$. 在(30)式的右边利用此式，我们得

$$(31)\quad \sum_{p\leq x}\frac{1}{p}=\frac{\log x+O(1)}{\log x}+\int_2^x\frac{\log t+R(t)}{t\log^2 t}dt$$

$$=1+O\left(\frac{1}{\log x}\right)+\int_2^x\frac{dt}{t\log t}$$

$$+\int_2^x\frac{R(t)}{t\log^2 t}dt,$$

而

$$\int_2^x\frac{dt}{t\log t}\log\log x-\log\log 2,$$

$$\int_2^x\frac{R(t)}{t\log^2 t}dt=\int_2^\infty\frac{R(t)}{t\log^2 t}dt-\int_x^\infty\frac{R(t)}{t\log^2 t}dt.$$

由条件$R(t)=O(1)$，这个广义积分的存在性是肯定的. 但是

$$\int_x^\infty\frac{R(t)}{t\log^2 t}dt=O\left(\int_x^\infty\frac{dt}{t\log^2 t}\right)=O\left(\frac{1}{\log x}\right).$$

于是等式(31)能改写为

$$\sum_{p\leq x}\frac{1}{p}=\log\log x+1-\log\log 2+\int_2^\infty\frac{R(t)}{t\log^2 t}dt$$

$$+O\left(\frac{1}{\log x}\right).$$

取

$$A=1-\log\log 2+\int_x^\infty\frac{R(t)}{t\log^2 t}dt,$$

定理得证. □

4.9 Möbius函数的部分和

定义　如果$x\geq 1$，我们定义

$$M(x)=\sum_{n\leq x}\mu(n).$$

$M(x)$的量值的准确的阶还不知道．数字的迹象暗示

$$|M(x)|<\sqrt{x}\qquad 如果x>1,$$

这个不等式通常称为Merten猜想，它没有被证明也无反例．至今得到的最好的O一结果是

$$M(x)=O(x\delta(x)),$$

这里$\delta(x)=\exp\{-A\log^{\frac{3}{5}}x(\log\log x)^{-\frac{1}{5}}\}$对某个正的常数A．（在Walfisz[75]里有一个证明）．

本节我们证明一个弱的结果，

$$\lim_{x\to\infty}\frac{M(x)}{x}=0$$

等价于素数定理．首先我们把$M(x)$与$\mu(n)$的另一个加权平均值联系起来．

定义　如果$x>1$，我们定义

$$H(x)=\sum_{n\leq x}\mu(n)\log n.$$

下面的定理说明$\frac{M(x)}{x}$的变化情况是由$\frac{H(x)}{(x\log x)}$确定的．

定理4.13　我们有

$$(32)\quad \lim_{x\to\infty}\left(\frac{M(x)}{x}-\frac{H(x)}{x\log x}\right)=0.$$

证明　在定理4.2里取$f(t)=\log t$，我们得

$$H(x)=\sum_{n\leqslant x}\mu(n)\log n=M(x)\log x-\int_1^x\frac{M(t)}{t}dt.$$

于是，当$x>1$时我们有

$$\frac{M(x)}{x}-\frac{H(x)}{x\log x}=\frac{1}{x\log x}\int_1^x\frac{M(t)}{t}dt.$$

为证明这个定理，我们必须证明

$$(33)\quad \lim_{x\to\infty}\frac{1}{x\log x}\int_1^x\frac{M(t)}{t}dt=0.$$

但我们有平凡的估计式$M(x)=O(x)$，所以，

$$\int_1^x\frac{M(t)}{t}dt=O\left(\int_1^x dt\right)=O(x),$$

由此得(33)，于是得(32)。

定理4.14　如果素数定理是成立的，则有

$$\lim_{x\to\infty}\frac{M(x)}{x}=0.$$

证明　我们利用$\psi(x)\sim x$形式的素数定理，并证明当$x\to\infty$时，$\frac{H(x)}{(x\log x)}\to 0$．为此我们需要等式

$$(34)\quad -H(x)=-\sum_{n\leqslant x}\mu(n)\log n=\sum_{n\leqslant x}\mu(n)\psi\left(\frac{x}{n}\right).$$

为证明(34)，我们从定理2.11着手．定理2.11说明

$$\Lambda(n)=-\sum_{d\mid n}\mu(d)\log d.$$

利用Möbius反转公式得

$$-\mu(n)\log n=\sum_{d\mid n}\mu(d)\Lambda\left(\frac{n}{d}\right).$$

对所有的$n\leqslant x$求和，并利用定理3.10，当$f=\mu$，$g=\Lambda$时，我们得到(34)．

因为$\psi(x)\sim x$，当$\varepsilon>0$是给定的时，存在一个常数$A>0$，

使得

$$\left|\frac{\psi(x)}{x}-1\right|<\varepsilon \quad 当x\geqslant A时.$$

换言之，我们有

$$(35)\quad |\psi(x)-x|<\varepsilon x \quad 当x\geqslant A时.$$

选取$x>A$并把(34)右端的和分为两部分

$$\sum_{n\leqslant y}+\sum_{y<n\leqslant x},$$

其中$y=\left[\frac{x}{A}\right]$. 在前一个和里，$n\leqslant y$，所以$n\leqslant\frac{x}{A}$，于是$\frac{x}{n}\geqslant A$. 因此我们可利用(35)写

$$\left|\psi\left(\frac{x}{n}\right)-\frac{x}{n}\right|<\varepsilon\frac{x}{n} \quad 当n\leqslant y时.$$

于是，

$$\sum_{n\leqslant y}\mu(n)\psi\left(\frac{x}{n}\right)=\sum_{n\leqslant y}\mu(n)\left(\frac{x}{n}+\psi\left(\frac{x}{n}\right)-\frac{x}{n}\right)$$

$$=x\sum_{n<y}\frac{\mu(n)}{n}+\sum_{n\leqslant y}\mu(n)\left(\psi\left(\frac{x}{n}\right)-\frac{x}{n}\right),$$

所以

$$\left|\sum_{n\leqslant y}\mu(n)\psi\left(\frac{x}{n}\right)\right|\leqslant x\left|\sum_{n\leqslant y}\frac{\mu(n)}{n}\right|$$

$$+\sum_{n\leqslant y}\left|\psi\left(\frac{n}{x}\right)-\frac{x}{n}\right|$$

$$<x+\varepsilon\sum_{n\leqslant y}\frac{x}{n}$$

$$<x+\varepsilon x(1+\log y)$$

$$<x+\varepsilon x+\varepsilon x\log x.$$

在第二个和里，我们有$y<n\leqslant x$，所以$n\geqslant y+1$，于是

$$\frac{x}{n}\leqslant\frac{x}{y+1}<A,$$

因为

$$y\leqslant\frac{x}{A}<y+1.$$

不等式$\left(\frac{x}{n}\right)<A$ 即$\psi\left(\frac{x}{n}\right)\leqslant\psi(A)$，因此第二个和不超过$x\psi(A)$，于是(34)的全部和不超过

$$(1+\varepsilon)x+\varepsilon x\log x+x\psi(A)<(2+\psi(A))x+\varepsilon x\log x$$

当$\varepsilon<1$时．换言之，给定任一ε，使$0<\varepsilon<1$，则有

$$|H(x)|<(2+\psi(A))x+\varepsilon x\log x \quad 当x>A时.$$

或者

$$\frac{|H(x)|}{x\log x}<\frac{2+\psi(A)}{\log x}+\varepsilon.$$

选取$B>A$，所以$x>B$推出$\frac{(2+\psi(A))}{\log x}<\varepsilon$．于是，对$x>B$，我们有

$$\frac{|H(x)|}{x\log x}<2\varepsilon,$$

它证明了，当$x\to\infty$时，$\frac{H(x)}{(x\log x)}\to 0.$ □

下面我们回到定理4.14的逆，并证明关系式

$$(36)\quad \lim_{x\to\infty}\frac{M(x)}{x}=0$$

能推出素数定理．首先我们引出“小o”符号．

定理 符号

$f(x)=o(g(x))$ 当$x\to\infty$时（读作：$f(x)$是$g(x)$的小o）意指

$$\lim_{x\to\infty}\frac{f(x)}{g(x)}=0.$$

这种形式的一个等式

$$f(x)=h(x)+o(g(x)) \quad 当x\to\infty时$$

意即$f(x)-h(x)=o(g(x))$　当$x\to\infty$时.

这样，(36)式即为

$$M(x)=o(x) \quad 当x\to\infty时,$$

并且表为$\psi(x)\sim x$的素数定理也可写为

$$\psi(x)=x+o(x) \quad 当x\to\infty时.$$

更一般，渐近式

$$f(x)\sim g(x) \quad 当x\to\infty时$$

等价于

$$f(x)=g(x)+o(g(x)) \quad 当x\to\infty时.$$

我们还要注意，$f(x)=O(1)$推出$f(x)=o(x)$当$x\to\infty$时.

定理4.15　关系式

$$(37)\quad M(x)=o(x) \quad 当x\to\infty$$

推出$\psi(x)\sim x$　当$x\to\infty$时.

证明　首先，我们用这种形式的式子来表述$\psi(x)$

$$(38)\quad \psi(x)=x-\sum_{\substack{q,d\\ qd\leq x}}\mu(d)f(q)+O(1).$$

然后利用(37)去证明其中和式是$o(x)$当$x\to\infty$时. (38)里的函数f由

$$f(n)=\sigma_0(n)-\log n-2C$$

给定，其中C是Euler常数，$\sigma_0(n)=d(n)$是n的约数的个数. 为得到(38)，首先我们有等式

$$[x]=\sum_{n\leq x}1,\quad \psi(x)=\sum_{n\leq x}\Lambda(n),\quad 1=\sum_{n\leq x}\left[\frac{1}{n}\right],$$

并把每一个加数表述为包含Möbius函数的Dirichlet乘积，

$$1=\sum_{d\mid n}\mu(d)\sigma_0\left(\frac{n}{d}\right),\quad \Lambda(n)=\sum_{d\mid n}\mu(d)\log\frac{n}{d},$$

$$\left[\frac{1}{n}\right]=\sum_{d\mid n}\mu(d).$$

故有

$$[x]-\psi(x)-2C=\sum_{n\leqslant x}\left\{1-\Lambda(n)-2C\left[\frac{1}{n}\right]\right\}$$

$$=\sum_{n\leqslant x}\ \sum_{d\mid n}\mu(d)\left\{\sigma_0\left(\frac{n}{d}\right)\right.$$

$$\left.-\log\frac{n}{d}-2C\right\}$$

$$=\sum_{\substack{q,\,d\\ qd\leqslant x}}\mu(d)\{\sigma_0(q)-\log q-2C\}$$

$$=\sum_{\substack{q,\,d\\ qd\leqslant x}}\mu(d)f(q).$$

这就推出(38). 因此，如果我们能证明

$$(39)\qquad \sum_{\substack{q,\,d\\ qd\leqslant x}}\mu(d)f(q)=o(x)\quad \text{当}x\to\infty\text{时},$$

定理的证明就完成了.

为此，我们利用定理3.17，写

$$(40)\qquad \sum_{\substack{q,\,d\\ qd\leqslant x}}\mu(d)f(q)=\sum_{n\leqslant b}\mu(n)F\left(\frac{x}{n}\right)$$

$$+\sum_{n\leqslant a}f(n)M\left(\frac{x}{n}\right)-F(a)M(b),$$

其中a与b是任一正数，使得ab=x且

$$F(x)=\sum_{n\leqslant x}f(n).$$

下面我们利用Dirichlet公式（定理3.3）

$$\sum_{n\leqslant x}\sigma_0(n)=x\log x+(2c-1)x+O(\sqrt{x})$$

与关系式

$$\sum_{n\leqslant x}\log n=\log[x]!\ =x\log x-x+O(\log x)$$

去证明 $F(x)=O(\sqrt{x})$.

这给我们

$$F(x)=\sum_{n\leqslant x}\sigma_0(n)-\sum_{n\leqslant x}\log n-2C\sum_{n\leqslant x}1$$

$$=x\log x+(2C-1)x+O(\sqrt{x})-(x\log x-x+O(\log x))-2Cx+O(1)$$

$$=O(\sqrt{x})+O(\log x)+O(1)=O+(\sqrt{x}).$$

因此，存在一个常数$B\geqslant 0$，使得

$$|F(x)|\leqslant B\sqrt{x}\quad 对所有x\geqslant 1.$$

在(40)式右边第一个和式里利用上式，得

$$(40)\quad \left|\sum_{n<b}\mu(n)F\left(\frac{x}{n}\right)\right|\leqslant B\sum_{n\leqslant b}\sqrt{\frac{x}{n}}\leqslant A\sqrt{xb}$$

$$=\frac{Ax}{\sqrt{a}}$$

对某个常数$A>B>0$.

现在令$\varepsilon>0$是任意的，并选$a>1$，使得

$$\frac{A}{\sqrt{a}}<\varepsilon,$$

于是(41)变为

$$(42)\quad \left|\sum_{n\leqslant b}\mu(n)F\left(\frac{x}{n}\right)\right|<\varepsilon x\quad 对所有的x\geqslant 1.$$

注意，a依赖于ε而与x无关.

因为$M(x)=O(x)$ 当$x\to\infty$时. 所以，对同一个ε，存在$c>0$（只依赖于ε），使得

$x>c$ 推出 $\frac{|M(x)|}{x}<\frac{\varepsilon}{K}$，

其中K是任一正数．（不久我们将指定K．）(40)式右边的第二个和式满足

$$(43)\quad \left|\sum_{n\leq a} f(n)M\left(\frac{x}{n}\right)\right| \leq \sum_{n\leq a}\left|f(n)\right|\frac{\varepsilon}{K}\cdot\frac{x}{n} = \frac{\varepsilon x}{K}\sum_{n\leq a}\frac{|f(n)|}{n}$$

如果对所有的 $n\leq a$ 有 $\frac{x}{n}>C$ 的话．因此，当 $x>ac$ 时，(43)成立．现在取

$$K=\sum_{n\leq a}\frac{|f(n)|}{n}.$$

于是(43)推出

$$(44)\quad \left|\sum_{n\leq a} f(n)M\left(\frac{x}{n}\right)\right| < \varepsilon x \quad 假如 x>ac.$$

假如 $\sqrt{x}>a$ 或 $x>a^2$ 的话，(40)式右边最后一项有界

$$\begin{aligned}|F(a)M(b)| &\leq A\sqrt{a}\,|M(b)| < A\sqrt{a}\,b\\ &<\varepsilon\sqrt{b}\,\sqrt{a}\,b\\ &=\varepsilon\sqrt{x}\,b<\varepsilon x.\end{aligned}$$

结合此结果与(44)，(42)，我们得到，由(40)推出

$$\left|\sum_{\substack{q,d\\ qd\leq x}}\mu(d)f(q)\right|<3\varepsilon x$$

假如 $x>a^2$ 与 $x>ac$，这里a与c只依赖于ε．这就证明了(39)．

定理4.16　如果

$$A(x)=\sum_{n\leq x}\frac{\mu(n)}{n},$$

那么，关系式

$$(45)\quad A(x)=O(1)\quad \text{当}x\to\infty\text{时}$$

推出素数定理．换言之，素数定理是级数

$$\sum_{n=1}^{\infty}\frac{\mu(n)}{n}$$

收敛且和为0这一论断的推论．

注：也能证明（参看[3]），素数定理推出这个级数收敛于0，所以(45)式实际上等价于素数定理．

证明　我们将证明(45)推出$M(x)=o(x)$．根据Abel等式，我们有

$$M(x)=\sum_{n\leqslant x}\mu(n)=\sum_{n\leqslant x}\frac{\mu(n)}{n}\cdot n$$
$$=xA(x)-\int_1^x A(t)dt,$$

所以

$$\frac{M(x)}{x}=A(x)-\frac{1}{x}\int_1^x A(t)dt.$$

为完成定理的证明，只要能证明

$$(46)\quad \lim\frac{1}{x}\int_1^x A(t)dt=0$$

就可以了．如果$\varepsilon>0$是给定的，则存在一个c，（仅依赖于ε）．使得$|A(x)|<\varepsilon$，当$x\geqslant c$时．因为对所有$x\geqslant1$，有$|A(x)|\leqslant1$，所以有

$$\left|\frac{1}{x}\int_1^x A(t)dt\right|\leqslant\left|\frac{1}{x}\int_1^c A(t)dt\right|$$
$$+\left|\frac{1}{x}\int_c^x A(t)dt\right|\leqslant\frac{c-1}{x}+\frac{\varepsilon(x-c)}{x}.$$

令$x\to\infty$，我们得到

$$\lim_{x\to\infty}\left|\frac{1}{x}\int_1^x A(t)dt\right|\leqslant\varepsilon,$$

因为ε是任意的，所以这证明了(46). □

4.10 素数定理初等证明的简短概要

本节给出素数定理初等证明的一个极简短的梗概，完全的详细证明可在[31]或[46]里得到. 这个证明的关键是Selberg渐近公式

$$\psi(x)\log x+\sum_{n\leqslant x}\Lambda(n)\psi\left(\frac{x}{n}\right)=2x\log x+O(x),$$

其证明是相对的简单并在下一节给出.本节是概括由Selberg公式推出素数定理的主要步骤.

首先，Selberg公式有一个更方便的计算公式，它包含函数

$$\sigma(x)=e^{-x}\psi(e^x)-1.$$

Selberg公式推出一个积分不等式

$$(47)\qquad |\sigma(x)|x^2\leqslant 2\int_0^x\int_0^y|\sigma(u)|dudy+O(x),$$

且素数定理等价于 $\sigma(x)\to 0$ 当$x\to\infty$时. 因此如果我们令

$$C=\limsup_{x\to\infty}|\sigma(x)|,$$

则素数定理相当于说$C=0$. 这由假设$C>0$并得到如下一个矛盾所证明. 由C的定义我们有

$$(48)\qquad |\sigma(x)|\leqslant C+g(x),$$

这里$g(x)\to 0$当$x\to\infty$时. 如果$C>0$，这个不等式与(47)一起，给出同一类型的另一个不等式

(49) $\quad |\sigma(x)| \leqslant C' + h(x)$,

这里$0 < C' < C$，并且当$x \to \infty$时，$h(x) \to 0$. 由(47)，(48)推出(49)是这个证明中最长的部分.在(49)里，令$x \to \infty$，我们得到$C \leqslant C'$，这是一个矛盾. 证明完成.

4.11 Selberg渐近公式

我们用Tatuzawa与Iseki[68]在1951年给出的方法推导Selberg公式. 它以下面的定理为基础，此定理具有一个反转公式的性质.

定理4.17 令F是一个定义在(0，∞)上的实值或复值函数，并令

$$G(x) = \log x \sum_{n \leqslant x} F\left(\frac{x}{n}\right),$$

则有

$$F(x)\log x + \sum_{n \leqslant x} F\left(\frac{x}{n}\right)\Lambda(n) = \sum_{d \leqslant x} \mu(d) G\left(\frac{x}{d}\right).$$

证明 首先，我们把$F(x)\log x$写为和式

$$F(x)\log x = \sum_{n \leqslant x}\left[\frac{1}{n}\right]F\left(\frac{x}{n}\right)\log\frac{x}{n}$$

$$= \sum_{n \leqslant x} F\left(\frac{x}{n}\right)\log\frac{x}{n}\sum_{d \mid n}\mu(d),$$

然后我们利用定理2.11的等式

$$\Lambda(n) = \sum_{d - x}\mu(d)\log\frac{n}{d}$$

去写

$$\sum_{n \leqslant x}F\left(\frac{x}{n}\right)\Lambda(n) = \sum_{n \leqslant x}F\left(\frac{x}{n}\right)\sum_{d \mid n}\mu(d)\log\frac{n}{d}.$$

这些等式相加，我们得

$$F(x)\log x+\sum_{n\leq x}F\left(\frac{x}{n}\right)\Lambda(n)$$

$$=\sum_{n\leq x}F\left(\frac{x}{n}\right)\sum_{d\mid n}\mu(d)\left\{\log\frac{x}{n}+\log\frac{n}{d}\right\}$$

$$=\sum_{n\leq x}\sum_{d\mid n}F\left(\frac{x}{n}\right)\mu(d)\log\frac{x}{d},$$

在最后的和式里，我们写$n=qd$，得

$$\sum_{n\leq x}\sum_{d\mid n}F\left(\frac{x}{n}\right)\mu(d)\log\frac{x}{d}$$

$$=\sum_{d\leq x}\mu(d)\log\frac{x}{d}\sum_{q\leq\frac{x}{d}}F\left(\frac{x}{qd}\right)=\sum_{d\leq x}\mu(d)G\left(\frac{x}{d}\right),$$

定理得证.

定理4.18 Selberg渐近公式．对$x>0$，我们有

$$\psi(x)\log x+\sum_{n\leq x}\Lambda(n)\psi\left(\frac{x}{n}\right)=2x\log x+O(x).$$

证明　我们对函数$F_1(x)=\psi(x)$与$F_2(x)=x-C-1$应用定理4.17，这里C是Euler常数．对应于F_1我们有

$$G_1(x)=\log x\sum_{n\leq x}\psi\left(\frac{x}{n}\right)$$

$$=x\log^2x-x\log x+O(\log^2x),$$

这里我们利用了定理4.11．对应于F_2我们有

$$G_2(x)=\log x\sum_{n\leq x}F_2\left(\frac{x}{n}\right)=\log x\sum_{n\leq x}\left(\frac{x}{n}-C-1\right)$$

$$=x\log x\sum_{n\leq x}\frac{1}{n}-(C+1)\log x\sum_{n\leq x}1$$

$$=x\log x\left(\log x+C+O\left(\frac{1}{x}\right)\right)$$

$$-(C+1)\log x(x+O(1))$$

$$=x\log^2 x-x\log x+O(\log x).$$

比较$G_1(x)$与$G_2(x)$的这两个公式，我们得 $G_1(x)-G_2(x)=O(\log^2 x)$. 实际上我们只须用弱的估计

$$G_1(x)-G_2(x)=O(\sqrt{x}).$$

现在我们对每一个F_1与F_2应用定理4.17 并把得到的两个关系式相减，二式右边的差是

$$\sum_{d\leq x}\mu(d)\left\{G_1\left(\frac{x}{d}\right)-G_2\left(\frac{x}{d}\right)\right\}$$

$$=O\left(\sum_{d\leq x}\sqrt{\frac{x}{d}}\right)=O\left(\sqrt{x}\sum_{d\leq x}\frac{1}{\sqrt{d}}\right)$$

$$=O(x),$$

这里用了定理3.2(b). 因此二式左边的差也是 $O(x)$. 换言之，我们有

$$\{\psi(x)-(x-C-1)\}\log x$$

$$+\sum_{n\leq x}\left\{\psi\left(\frac{x}{n}\right)-\left(\frac{x}{n}-C-1\right)\right\}\Lambda(n)=O(x).$$

重排这些项并利用定理4.9，我们得

$$\psi(x)\log x+\sum_{n\leq x}\psi\left(\frac{x}{n}\right)\Lambda(n)$$

$$=(x-C-1)\log x+\sum_{n\leq x}\left(\frac{x}{n}-C-1\right)\Lambda(n)+O(x)$$

$$=2x\log x+O(x).$$ □

第四章习题

1. 令$S=\{1, 5, 9, 13, 17, \cdots\}$表示$4n+1$形式的所有正整数的集合. S的元素p称为是S—素数，当$p>1$且p在

S中的约数只有1与p时．（例如49就是一个S—素数．）S中的元素$n>1$不是S—素数就称为S—复合数．

(a) 证明每一个S—复合数是S—素数的乘积．

(b) 找出一个最小的S—复合数，它能以多于一种方式表为S—素数的乘积．

这说明在S里因子分解式的唯一性不成立．

2．讨论下面的整数的有限集合

$$T=\{1, 7, 11, 13, 17, 19, 23, 29\}.$$

(a) 对于在区间$30<P<100$里的每一个素数p，确定一对整数m，n，其中$m\geqslant 0$，$n\in T$，使得

$$p=30m+n.$$

(b) 证明下面的论述或举出一个反例：

每一个素数$p>5$能表为$30m+n$的形式，其中$m\geqslant 0$且$n\in T$．

3．令$f(x)=x^2+x+41$，找出最小的整数$x\geqslant 0$，对于这个整数，$f(x)$是复合数．

4．令$f(x)=q_0+q_1x+\cdots+q_nx^n$是一个整系数多项式，这里$a_n>0$且$n\geqslant 1$．证明，有无穷多个整数x，使$f(x)$是复合数．

5．证明，对每一个$n\geqslant 1$，存在n个连续复合数．

6．证明，不存在多项p式Q与，使得

$$\pi(x)=\frac{p(x)}{Q(x)} \qquad 对x=1, 2, 3, \cdots.$$

7．令$a_1<a_2<\cdots<a_n\leqslant x$是一个正整数集合，其中没有$a_i$能整除其它的数的乘积，证明，$n\leqslant\pi(x)$．

8．计算能整除$1000!$的10的最高方幂．

9. 给定整数的一个等差级数

$h, h+k, h+2k, \cdots, h+nk, \cdots$

其中$0<k<2000$. 如果对$n=t, t+1, \cdots, t+r$, $h+nk$是素数, 证明$r\leqslant 9$, 换言之, 这个级数最多只有连续10项是素数.

10. 令S_n表示级数$\sum_{r=1}^{\infty}\frac{1}{r(r+1)}$的前n项的部分和, 证明, 对每一个整数$k>1$, 存在整数m与n, 使得

$$S_m-S_n=\frac{1}{K}.$$

11. 令S_n表示前n个素数之和. 证明, 对每一个n, 存在一个整数, 其平方位于S_n与S_{n+1}之间.

证明12至16题的每一题. 在这些题里, 你可以利用素数定理.

12. 如果$a>0$, $b>0$, 则$\frac{\pi(ax)}{\pi(bx)}\sim\frac{a}{b}$, 当$x\to\infty$时.

13. 如果$0<a<b$, 则存在x_0, 使得$\pi(ax)<\pi(bx)$, 当$x\geqslant x_0$时.

14. 如果$0<a<b$, 则存在一个x_0, 使得对$x\geqslant x_0$, 在ax与bx之间至少有一个素数.

15. 每一个区间$[a, b]$, $0<a<b$, 一定包含一个$\frac{p}{q}$形式的有理数, 这里p与q都是素数.

16. (a) 给定一个正整数n, 则存在一个正整数K与一个素数p, 使得

$10^K n<p<10^K(n+1)$

(b) 给定m个整数$a_1, a_2, \cdots, a_m$, 满足$0<a_i<9$, 对$i=1, 2, \cdots, m$. 则存在一个素数p, 它的十进位

数展开式的前m个数码是a_1，a_2，…，a_m.

17．给定一个整数$n\geqslant 1$，它有两个因子分解式$n=\prod_{i=1}^{r} p_i$与$n=\prod_{i=1}^{t} q_i$，其中p_i是素数（可以相同）而q_i是任意>1的整数．令α是一个非负实数.

(a) 如果$\alpha\geqslant 1$，证明

$$\sum_{i=1}^{r} p_i^{\alpha}\leqslant\sum_{i=1}^{t} q_i^{\alpha}.$$

(b) 如果$0\leqslant\alpha<1$，求出关于这两个和式的相应的不等式.

18．证明，下面两个式子是等价的：

(a) $\pi(x)=\dfrac{x}{\log x}+O\left(\dfrac{x}{\log^2 x}\right)$.

(b) $g(x)=x+O\left(\dfrac{x}{\log x}\right)$.

19．如果$x\geqslant 2$，令

$$Li(x)=\int_2^x\frac{dt}{\log t}\ (x\text{的对数积分}).$$

(a) 证明

$$Li(x)=\frac{x}{\log x}+\int_2^x\frac{dt}{\log^2 t}-\frac{2}{\log 2},$$

更一般

$$Li(x)=\frac{x}{\log x}\left(1+\sum_{K=1}^{n-1}\frac{K!}{\log^K x}\right)+n!\int_2^x\frac{dt}{\log^{n+1}t}+C_n,$$

其中C_n与x无关.

(b) 如果$x\geqslant 2$，证明

$$\int_2^x \frac{dt}{\log^n t} = O\left(\frac{x}{\log^n x}\right).$$

20．令f是一个数论函数，满足

$$\sum_{p\leqslant x} f(p)\log p = (ax+b)\log x + cx + O(1) \quad 对x\geqslant 2.$$

证明，有一个常数A（依赖于f），使得，如果 $x\geqslant 2$，则有

$$\sum_{p\leqslant x} f(p) = ax + (a+c)\left(\frac{x}{\log x} + \int_2^x \frac{dt}{\log^2 t}\right)$$

$$+ b\log(\log x) + A + O\left(\frac{1}{\log x}\right).$$

21．已知两个实值函数S(x)与T(x)，满足

$$T(x) = \sum_{n\leqslant x} S\left(\frac{x}{n}\right) \quad 对所有x\geqslant 1.$$

如果 $S(x)=O(x)$ 且C是一个正的常数　证明，

$S(x)\sim Cx$　当 $x\to\infty$ 时

可推出

$T(x)\sim Cx\log x$　当 $x\to\infty$ 时.

22．证明，定理4.18中表述的Selberg公式与下面关系式中的每一个等价.

(a) $\psi(x)\log x + \sum_{p\leqslant x} \psi\left(\frac{x}{p}\right)\log p = 2x\log x + O(x).$

(b) $g(x)\log x + \sum_{p\leqslant x} g\left(\frac{x}{p}\right)\log p = 2x\log x + O(x).$

23．令 $M(x) = \sum_{n\leqslant x} \mu(n)$．证明

$$M(x)\log x + \sum_{n\leqslant x} M\left(\frac{x}{n}\right)\Lambda(n) + O(x)$$

与

$$M(x)\log x + \sum_{p\leqslant x} M\left(\frac{x}{p}\right)\log p = O(x).$$

[提示：定理4.17]

24. 令A(x)对所有的x>0有定义，并假设

$$T(x)=\sum_{n\leq x}A\left(\frac{x}{n}\right)=ax\log x+bx+O\left(\frac{x}{\log x}\right)$$

当$x\to\infty$时。

其中a与b是常数，证明

$$A(x)\log x+\sum_{n\leq x}A\left(\frac{x}{n}\right)\Lambda(n)=2ax\log x+0(x\log x)$$

$x\to\infty$.

并验证定理4.18中的Selberg公式是此式的一个特殊情形.

25. 证明，形如$\psi(x)\sim x$的素数定理可以推出定理4.18中的Selberg公式而误差项为$0(x\log x)$　$x\to\infty$.

26. 1851年Chebyshev曾证明，如果$x\to\infty$时，$\frac{\psi(x)}{x}$趋于一个极限，那么这个极限等于1．本题概括了以公式

(50) $\sum_{n\leq x}\psi\left(\frac{x}{n}\right)=x\log x+O(x)$

为基础的这个结果的一个简单的证明．(50)是由定理4.11得出的.

(a) 令$\delta=\limsup_{x\to\infty}\left(\frac{\psi(x)}{x}\right)$. 给定$\varepsilon>0$，选择$N=N(\varepsilon)$，使得$x\geq N$推出$\psi(x)\leq(\delta+\varepsilon)x$. 把(50)里的和分为两部分，一部分为$n\leq\frac{x}{N}$，另一部分为$n>\frac{x}{N}$，并估计每一部分得不等式

$$\sum_{n\leq x}\psi\left(\frac{x}{n}\right)\leq(\delta+\varepsilon)x\log x+x\psi(N),$$

把此式与(50)比较，推出$\delta\geq1$.

(b) 令$r=\liminf\limits_{x\to\infty}\left(\frac{\psi(x)}{x}\right)$并利用与(a)类似的理由推导出$r\leqslant1$. 因此，当$x\to\infty$时，如果$\frac{\psi(x)}{x}$有一个极限，则$r=\delta=1$.

在27至30题中，令$A(x)=\sum\limits_{n\leqslant x}a(n)$，其中$a(n)$满足

(51) $a(n)\geqslant0$ 对所有$n\geqslant1$，与

(52) $\sum\limits_{n\leqslant x}A\left(\frac{x}{n}\right)=\sum\limits_{n\leqslant x}a(n)\left[\frac{x}{n}\right]$

$$=ax\log x+bx+O\left(\frac{x}{\log x}\right)$$

$x\to\infty$.

当$a(n)=\Lambda(n)$时，这些式子里的$a=1$，$b=-1$. 下面的习题证明，(51)与(52)以及素数定理$\psi(x)\sim x$可推出$A(x)\sim ax$. 这将与定理4.8比较（Shapiro Tauberian定理），这里只假设(51)与弱的条件$\sum\limits_{n\leqslant x}A\left(\frac{x}{n}\right)=ax\log x+O(x)$并且断定$Cx\leqslant A(x)\leqslant B(x)$对某些正的常数C与B.

27. 证明

(a) $\sum\limits_{n\leqslant x}A\left(\frac{x}{n}\right)\Lambda(n)$

$$=\sum_{n\leqslant\sqrt{x}}A\left(\frac{x}{n}\right)+\sum_{n\leqslant\sqrt{x}}\psi\left(\frac{x}{n}\right)a(n)+O(x),$$

利用此式推导关系式

(b) $\frac{A(x)}{x}+\frac{1}{x\log x}\sum\limits_{n\leqslant\sqrt{x}}A\left(\frac{x}{n}\right)\Lambda(n)$

$$+\frac{1}{x\log x}\sum_{n\leqslant\sqrt{x}}\psi\left(\frac{x}{n}\right)a(n)$$
$$=2a+O(1).$$

28. 令$\alpha=\liminf\limits_{x\to\infty}\left(\frac{A(x)}{x}\right)$，$\beta=\limsup\limits_{x\to\infty}\left(\frac{A(x)}{x}\right)$，

(a) 选取任意的$\varepsilon>0$，利用事实

$$A\left(\frac{x}{t}\right)<(\beta+\varepsilon)\frac{x}{t}\ \text{与}\ \psi\left(\frac{x}{t}\right)<(1+\varepsilon)\frac{x}{t}$$

对所有充分大的$\frac{x}{t}$成立，并利用27题(b)去导出

$$\alpha+\frac{\beta}{2}+\frac{a}{2}+\frac{\varepsilon}{2}+\frac{a\varepsilon}{2}>2a.$$

因为ε是任意的，这就推出

$$\alpha+\frac{\beta}{2}+\frac{a}{2}\geqslant 2a.$$

[提示：令$x\to\infty$，使$\frac{A(x)}{x}\to\alpha$.]

(b) 用类似的理由证明

$$\beta+\frac{\alpha}{2}+\frac{a}{2}\leqslant 2a,$$

并导出$\alpha=\beta=a$. 换言之，当$x\to\infty$时，$A(x)\sim ax$.

29. 取$a(n)=1+\mu(n)$并验证，当$a=1$，$b=2C-1$时，(52)式是满足的，这里C是Euler常数.
证明，由28题的结果可推出

$$\lim_{n\to\infty}\frac{1}{x}\sum\mu(n)=0.$$

这就给出定理4.14的一个替换证明.

30. 如果在28题里，我们不假定素数成立，代替的条件是设

$$r=\liminf_{x\to\infty}\frac{\psi(x)}{x},\quad \delta=\limsup_{x\to\infty}\frac{\psi(x)}{x},$$

(a) 证明，由(28)题的结果导出不等式

$$\alpha+\frac{\beta}{2}+\frac{a\delta}{2}\geqslant 2a,\quad \beta+\frac{\alpha}{2}+\frac{ar}{2}\leqslant 2a.$$

(b) 由(a) 的不等式证明

$$ar\leqslant\alpha\leqslant\beta\leqslant a\delta.$$

这说明，满足(51)与(52)的所有的数$a(n)$中，有一个固定的a，当$a(n)=a\Lambda(n)$时，两个最广泛的分离的极限

$$\liminf_{x\to\infty}\frac{A(x)}{x}\ 与\ \limsup_{x\to\infty}\frac{A(x)}{x}$$

不确定. 于是，对唯一特别情况$a(n)=a\Lambda(n)$，由(51)与(52)可导出$A(x)\sim ax$.

第五章　同　　余

5.1　同余的定义与基本性质

Gauss引入了一个著名的记号，这个记号简化了关于整数整除性的许多问题．这样，他创造了一个新的被称为同余理论的数论分支．本章讨论的是同余式的基础．

除非特别指出，小写的拉丁字母与希腊字母都表示整数．（正数，负数或零．）

定义　给定整数a，b与m，$m>0$，如果m整除差$a-b$，我们就说a，b对模m同余，记为

（1）$a\equiv b\ (\bmod m)$，

其中，数m称为模．

换言之，（1）等价于整除式

$$m\mid(a-b).$$

特别，当且仅当$m\mid a$时，$a\equiv 0(\bmod m)$，于是$a\equiv b(\bmod m)$当且仅当$a-b\equiv 0(\bmod m)$．如果$m\nmid(a-b)$，我们记为$a\not\equiv b(\bmod m)$，并说a与b对模m不同余．

例子：

1．$19\equiv 7\ (\bmod 12)$，$1\equiv -1\ (\bmod 2)$，$3^2\equiv -1$

(mod5).

2. n是偶数，当且仅当$n\equiv 0 \pmod 2$.

3. n是奇数，当且仅当$n\equiv 1 \pmod 2$.

4. $a\equiv d \pmod 1$对每个a与b都成立.

5. 如果$a\equiv b \pmod m$, $d\mid m$, $d>0$, 则有$a\equiv b \pmod d$.

同余符号≡是由Gauss 联想到类似于等号＝而提出的. 下面两个定理说明同余实际上具有许多与等式相似的性质.

定理5.1　同余是等价关系，就是说，我们有

(a) $a\equiv a \pmod m$　　（反身性）

(b) $a\equiv b \pmod m$推出$b\equiv a \pmod m$　　（对称性）

(c) $a\equiv b \pmod m$与$b\equiv c \pmod m$
推出$a\equiv c \pmod m$　　（传递性）

证明　这个证明由整除性立即得到.

(a) $m\mid 0$.

(b) 如果$m\mid (a-b)$，则有$m\mid (b-a)$.

(c) 如果$m\mid (a-b)$与$m\mid (b-c)$，则有$m\mid (a-b)+(b-c)=a-c$. □

定理5.2　如果$a\equiv b \pmod m$，$\alpha\equiv\beta \pmod m$，则有

(a) $ax+\alpha y\equiv bx+\beta y \pmod m$对所有的整数x与y.

(b) $a\alpha\equiv b\beta \pmod m$.

(c) $a^n\equiv b^n \pmod m$　　对每个正整数n.

(d) $f(a)\equiv f(b) \pmod m$　　对每个整系数多项式f.

证明　(a) 因为$m\mid (a-b)$，$m\mid (\alpha-\beta)$，所以有

$$m\mid x(a-b)+y(\alpha-\beta)=(ax+\alpha y)-(bx+\beta y).$$

(b) 注意到$a\alpha-b\beta=\alpha(a-b)+b(\alpha-\beta)\equiv 0 \pmod m$ 根据(a).

(c) 在(b)里，取$\alpha=a$，$\beta=b$并对n作归纳法.

(d) 利用(c)并对f的次数作归纳法. □

定理5.2告诉我们，模相同的两个同余式的元素与元素能够相加、相减与相乘，就象它们是等式一样. 对于模相同的任意有限多个同余式同样是正确的.

在进一步展开同余的性质之前我们给出两个例子以阐明它们的用处.

例1. 被9整除的检验. 一个整数$n>0$被9整除当且仅当它的十进位制数的各位数字之和被9整除. 利用同余，这个性质容易证明. 如果n的十进位制数的各位数字记为a_0，a_1，…，a_k，则

$$n=a_0+10a_1+10^2a_2+\cdots+10^ka_k.$$

利用定理5.2，模为9，我们有

$$10\equiv1,\ 10^2\equiv1,\ \cdots,\ 10^k\equiv1\ (\mathrm{mod}\,9),$$

所以

$$n\equiv a_0+a_1+\cdots+a_k\quad(\mathrm{mod}\,9).$$

注意，所有这些式子对模3同样是成立的，所以一个数被3整除当且仅当它的各位数字之和被3整除.

例2. Fermst数$F_n=2^{2^n}+1$是前面的历史介绍中提到过的. 前5个是$F_0=3$，$F_1=5$，$F_2=17$，$F_3=257$，$F_4=65537$都是素数. 现在，不用清楚地计算出F_5，就可以证明F_5被641整除. 为此，我们对模641逐次地讨论方幂2^{2^n}，我们有

$$2^2=4,\ 2^4=16,\ 2^8=256,\ 2^{16}\equiv65536\equiv154\ (\mathrm{mod}\,641).$$

所以，

$$2^{32}\equiv(154)^2=23716\equiv640\equiv-1\ (\mathrm{mod}\,641),$$

因此，$F_5=2^{32}+1\equiv 0\pmod{641}$，故$F_5$是复合数.

现在我们回到同余的一般性质．非零的公因子不能像等式那样从同余式的两端消去．

例如．

$$48\equiv 18\pmod{10}$$

的两边的元素都能被6整除，但若我们消去公因子6，我们就得到一个错误的结果$8\equiv 3\pmod{10}$．下面的定理说明，如果模也能被这个公因子整除，则公因子可以消去．

定理5.3　如果$c>0$，则

$a\equiv b\pmod{m}$当且仅当$ac\equiv bc\pmod{mc}$．

证明　我们有$m\mid(b-a)$当且仅当$cm\mid(cb-ca)$．　□

下面的定理叙述消去律，当模不能被公因子整除时，消去律可以使用．

定理5.4　消去律．如果$ac\equiv bc\pmod{m}$并且$d=(m,c)$，则

$$a\equiv b\quad\left(\bmod\ \frac{m}{d}\right).$$

换言之，，假若模也被$d=(m,c)$整除，则公因子c能够消去．

证明　因为$ac\equiv bc\pmod{m}$，我们有

$$m\mid c(a-b)\text{，所以}\frac{m}{d}\ \Big|\ \frac{c}{d}(a-b).$$

但是$\left(\frac{m}{d},\ \frac{c}{d}\right)=1$，于是有$\frac{m}{d}\ \Big|\ (a-b)$．　□

定理5.5　假设$a\equiv b\pmod{m}$．如果$d\mid m$，$d\mid a$，那么有$d\mid b$．

证明　不妨设$d>0$．如果$d\mid m$，则由$a\equiv b\pmod{m}$可

推出 $a\equiv b(\bmod d)$. 但若 $d|a$，则 $a\equiv 0(\bmod d)$，所以 $b\equiv 0$ $(\bmod d)$. □

定理5.6 如果 $a\equiv b(\bmod m)$，则 $(a,m)=(b,m)$. 换言之，对模m同余的二数与m有相同的最大公约数.

证明　令 $d=(a,m)$，$e=(b,m)$. 则 $d|m$，$d|a$，所以 $d|b$，因此 $d|e$. 同理，$e|m$，$e|b$，所以 $e|a$. 于是 $e|d$. 因此 $d=e$. □

定理5.7 如果 $a\equiv b(\bmod m)$ 且 $0\leqslant|b-a|<m$. 则有 $a=b$.

证明　因为 $m|(a-b)$，所以除非 $a-b=0$，我们有 $m\leqslant|a-b|$.

定理5.8 我们有，$a\equiv b(\bmod m)$ 当且仅当a与b被m除时有相同的余数.

证明　写 $a=mq+r$，$b=m\theta+R$，这里 $0\leqslant r<m$，$0\leqslant R<m$. 则有 $a-b\equiv r-R\ (\bmod m)$ 且 $0\leqslant|r-R|<m$，然后利用定理5.7即得.

定理5.9 如果 $a\equiv b(\bmod m)$ 且 $a\equiv b(\bmod n)$，其中 $(m,n)=1$. 则 $a\equiv b(\bmod mn)$.

证明　因为m与n二数都整除 $a-b$，并且 $(m,n)=1$，所以二数之积mn也整除 $a-b$. □

5.2 剩余类与完全剩余系

定义　考虑一个固定的 $m>0$，我们用 $\hat{a}$ 表示满足 $x\equiv a$ $(\bmod m)$ 的所有整数x的集合，我们称 $\hat{a}$ 是模m的一个剩余类.

这样，$\hat{a}$由形如$a+mq$的所有整数组成，这里的$q=0$，±1，±2，…．

下面的剩余类的性质是这个定义的很自然的推论．

定理5.10　对一个给定的模m，我们有

(a) $\hat{a}=\hat{b}$当且仅当$a\equiv b(\bmod m)$．

(b) 两个整数x与y属于同一类当且仅当

$x\equiv y(\bmod m)$．

(c) m个剩余类$\hat{1}$，$\hat{2}$，…，$\hat{m}$互不相交而它们的并就是全体整数的集合．

证明　(a)与(b)由定义立即得到．为证明(c)，我们注意0，1，2，…，$m-1$对模m是互不同余的．（据定理5.7）．由(b)，剩余类

$$\hat{0}，\hat{1}，\hat{2}，\cdots，\widehat{m-1}$$

是互不相交的．但每一个整数x一定要属于这些类中的一个确定的类里，这是因为$x=mq+r$，这里$0\leqslant r<m$，所以$x\equiv r(\bmod m)$　$x\in\hat{r}$．还因为$\hat{0}=\hat{m}$这就证明了(c)．　□

定义　由剩余类$\hat{1}$，$\hat{2}$，…，$\hat{m}$的每一类中的一个代表做成的m个代表的集合称为是模m的一个完全剩余系．

例子　任意m个对模不同余的整数集合都是模m的一个完全剩余系．例如

$$\{1，2，\cdots，m\}；\qquad\{0，1，2，\cdots，m-1\}；$$

$$\{1，m+2，2m+3，3m+4，\cdots，m^2\}．$$

定理5.11　设$(k，m)=1$，如果$\{a_1，\cdots，a_m\}$是模m的一个完全剩余系，则$\{ka_1，\cdots，ka_m\}$也是模m的一个完全剩余系．

证明　如果$ka_i \equiv ka_j \pmod{m}$，则有$a_i \equiv a_j \pmod{m}$，这因为$(k, m)=1$. 因此集合$\{ka_1, \cdots, ka_m\}$中没有两个元素对模m同余，又因此集合有m个元素，所以它组成一个完全剩余系. □

5.3　一次同余式

多项式同余式能与代数中的方程以相同的方法进行研究. 为了在x是整数时，多项式的值也是整数，所以我们论述的多项式$f(x)$都是整系数的. 一个整数x如果满足一个多项式同余式

（2）$f(x) \equiv 0 \pmod{m}$,

则x叫做是这个同余式的一个解. 当然，如果$x \equiv y \pmod{m}$，则$f(x) \equiv f(y) \pmod{m}$，所以一个同余式的一个解有无穷多个解. 因此，我们约定属于同一个剩余类的那些解是同一个解. 当我们谈到如（2）那样的同余式的解的个数的时候，我们指的是不同余的解的个数，也就是包含在集合$\{1, 2, \cdots, m\}$中或任一完全剩余系中的解的个数. 因此，模m的任一多项式同余式最多只有m个解.

例1.　一次同余式$2x \equiv 3 \pmod{4}$没有解. 因为$2x-3$对每个x都是奇数，因此不能被4整除.

例2.　二次同余式$x^2 \equiv 1 \pmod{8}$恰有4个解，由$x \equiv 1, 3, 5, 7 \pmod{8}$给出.

一次同余式的全部理论由下面三个定理所表述.

定理5.12　设$(a, m)=1$，则一次同余式

（3）$ax \equiv b \pmod{m}$

恰有一个解.

证明　我们只需检验1，2，…，m，因为它们组成一个完全剩余系. 因此，我们作乘积a，2a，…，ma，由于(a，m)＝1，所以这些数也组成一个完全剩余系，于是这些乘积中恰有一个与b同余，也就是恰有一个x满足(3). □

虽然定理5.12告诉我们，同余式(3)有唯一的一个解，但它除了检验完全剩余系中的所有的数之外，没有告诉我们如何去确定这个解. 有一些更简捷的著名的确定解的方法，它们将在本章的后面被论述.

注意，如果(a，m)=1，则同余式ax≡1(modm)的唯一解称为是a的倒数modm.如果a' 是a的倒数，则ba' 是(3)的解.

定理5.13　设(a，m)＝d，则一次同余式

(4)　$ax\equiv b(\mathrm{mod}\,m)$

有解当且仅当d|b.

证明　如果解存在，因为d|a与d|m，于是有d|b. 反之，如果d|b，则因$\left(\frac{a}{d},\ \frac{m}{d}\right)=1$，故同余式

$$\frac{a}{d}x\equiv\frac{b}{d}\quad\left(\mathrm{mod}\,\frac{m}{d}\right)$$

有一解，而这个解也是(4)的一个解. □

定理5.14　设(a，m)＝d，d|b，则同余式

(5)　$ax\equiv b\quad(\mathrm{mod}\,m)$

对模m恰有d个解，它们由

(6)　$t,\ t+\frac{m}{d},\ t+2\frac{m}{d},\ \cdots,\ t+(d-1)\frac{m}{d}$

给出，这里t是一次同余式

(7)　$\frac{a}{d}x\equiv\frac{b}{d}\quad\left(\mathrm{mod}\,\frac{m}{d}\right)$

的对模$\frac{m}{d}$的唯一解.

证明　(7)的每一个解也是(5)的解. 反之, (5)的每一个解也满足(7). 于是在(6)里列出的d个数都是(7)的解, 因而也是(5)的解. 但它们任何两个对模m都不同余, 因为由

$$t+r\frac{m}{d}\equiv t+s\frac{m}{d}\ (\mathrm{mod}\, m),\quad 0\leqslant r<d,\quad 0\leqslant s<d$$

导出

$$r\frac{m}{d}\equiv s\frac{m}{d}\ (\mathrm{mod}\, m)\qquad 于是 r\equiv s\left(\mathrm{mod}\,\frac{m}{d}\right).$$

但　$0\leqslant|r-s|<d$, 所以$r=s$.

余下证明, 除了(6)里列出的那些数之外, 同余式(5)没有其它的解. 如果y是(5)的一个解, 则$ay\equiv at\ (\mathrm{mod}\, m)$, 所以$y\equiv t\left(\mathrm{mod}\,\frac{m}{d}\right)$, 于是$y=t+k\frac{m}{d}$对某个k. 但$k\equiv r\ (\mathrm{mod}\, d)$对满足$0\leqslant r<d$的某个r. 因此

$$k\frac{m}{d}\equiv r\frac{m}{d}\ (\mathrm{mod}\, m),\ 所以 y\equiv t+k\frac{m}{d}\ (\mathrm{mod}\, m).$$

因此y与(6)中的一个数同余mod m. 证明完成. □

在第一章里, 我们证明了两个数a与b的最大公约数是a与b的一个线性组合. 作为定理5.14的一个推论能得出同样的结果.

定理5.15　如果$(a、b)=d$, 则存在整数x与y, 使得

(8)　$ax+by=d$.

证明　一次同余式$ax\equiv d(\mathrm{mod}\, b)$有一个解, 于是有一个整数y使得$d-ax=by$, $ax+by=d$. □

注：几何意义，满足(8)式的数对(x、y)是位于直线上的格点，这些格点的每一个的x坐标都是同余式$ax\equiv d(\mathrm{mod}\,b)$的解．

5.4 简化剩余系与Euler–Fermat定理

定义 所谓模m的一个简化剩余系是指$\varphi(m)$个整数的一个集合，这$\varphi(m)$个数对模m互不同余，其中每一个数都与m互素．

注：$\varphi(m)$是在第二章里介绍过的Euler函数．

定理5.16 如果$\{a_1, a_2, \cdots, a_{\varphi(m)}\}$是模m的一个简化剩余系，并且$(k, m)=1$，则$\{ka_1, ka_2, \cdots, ka_{\varphi(m)}\}$也是模m的一个简化剩余系．

证明 ka_i中任意两个对模m都不同余．又因为$(a_i, m)=(k, m)=1$，我们有$(ka_i, m)=1$，所以每一个ka_i都与m互素． □

定理5.17 Euler–Fermat定理．设$(a, m)=1$，则有

$$a^{\varphi(m)}\equiv 1 \quad (\mathrm{mod}\,m).$$

证明 设$\{b_1, b_2, \cdots, b_{\varphi(m)}\}$是模m的一个简化剩余系，则$\{ab_1, ab_2, \cdots, ab_{\varphi(m)}\}$也是模m的一个简化剩余系．于是第一个集合中所有整数之积与第二个集合中所有整数之积同余，因此有

$$b_1\cdots b_{\varphi(m)}\equiv a^{\varphi(m)}b_1\cdots b_{\varphi(m)} \quad (\mathrm{mod}\,m).$$

由于每一个b_i都与m互素，所以我们能够消去b_i而得到定理． □

定理5.18 如果一个素数p不能整除a，则

$$a^{p-1}\equiv 1 \quad (\mathrm{mod}\,p).$$

证明　因为$\varphi(p)=p-1$. 这是前一个定理的推论. □

定理5.19　Fermat小定理. 对任一整数a与任一素数p, 我们有

$$a^p \equiv a \pmod{p}.$$

证明　如果$p\nmid a$, 这就是定理5.18. 如果$p|a$, 则a^p与a二者都同余于0 mod p. □

Euler-Fermat定理能用于求一次同余式的解.

定理5.20　如果$(a, m)=1$, 则一次同余式

(9)　$ax\equiv b \pmod{m}$

的唯一解由

(10)　$x\equiv ba^{\varphi(m)-1} \pmod{m}$

给出.

证明　由Euler-Fermat定理,(10)给出的数x满足(9). 又因$(a, m)=1$. 这个解对模m是唯一的. □

例1.　解同余式　$5x\equiv 3 \pmod{24}$.

解.

因为$(5, 24)=1$, 所以有唯一解. 利用(10)得

$$x\equiv 3.5^{\varphi(24)-1}\equiv 3.5^7 \pmod{24},$$

这因为$\varphi(24)=\varphi(3)\varphi(8)=2.4$. 对于模24, 我们有

$$5^2\equiv 1,\ 5^4\equiv 5^6\equiv 1,\ 5^7\equiv 5,\ \text{所以} x\equiv 15 \pmod{24}.$$

例2.　解同余式　$25x\equiv 15 \pmod{120}$.

解.

因为$d=(25, 120)=5$且$d|15$, 所以此同余式对模120恰有5个解. 为了找到它们, 我们用5去除原式并解同余式$5x\equiv 3 \pmod{24}$. 利用例1与定理5.14, 我们得到这5个解为

$x=15+24k \qquad k=0,1,2,3,4$或者

$x\equiv 15, 39, 63, 87, 111 \pmod{120}$.

5.5 模p的多项式同余式.Lagrange定理

代数基本定理说明，每一个次数$n\geqslant 1$的多项式f 的方程$f(x)=0$在复数域中有n个解. 对于多项式同余式来说此定理恰好不能类推. 例如，我们曾看到，某些一次同余式没有解，某些一次同余式恰有一个解，而某些一次同余式有多于一个解. 因此，甚至在这样特殊的情形里，看来多项式的次数与同余式的解数之间没有简单的关系式. 但是，一个素数模的同余式却有下面的Lagrange定理.

定理5.21 (Lagrange). 给定一个素数P，令

$$f(x)=c_0+c_1x+\cdots c_nx^n$$

是一个n次整系数多项式，$c_n\not\equiv 0 \pmod{p}$，则多项式同余式

$$(11)\quad f(x)\equiv 0 \pmod{P}$$

最多只有n个解.

注意，这个结果对复合数模是不成立的.例如，二次同余式$x^2\equiv 1 \pmod{8}$有4个解.

证明　我们对f的次数n作归纳法. 当$n=1$时，这个同余式是一次的，

$$c_1x+c_0\equiv 0 \pmod{p}$$

因为$c_1\not\equiv 0 \pmod{p}$，我们有$(c_1, p)=1$，同余式恰有一解.

于是，假设这个定理对于次数为$n-1$的多项式是成立的，并设同余式(11)对模p有$n+1$个不同余的解，写为

$$x_0, \ x_1, \ \cdots, \ x_n.$$

这里，对每一个$k=0, 1, \cdots, n$，有$f(x_k)\equiv 0 \pmod{p}$，我们将会得到一个矛盾．我们有代数等式

$$f(x)-f(x_0)=\sum_{r=1}^{n}c_r(x^r-x_0^r)=(x-x_0)g(x),$$

其中$g(x)$是一个次数为$n-1$的整系数多项式，首项系数是c_n．于是我们有

$$f(x_k)-f(x_0)\equiv(x_k-x_0)g(x_k)\equiv 0 \pmod{p},$$

这因为$f(x_k)\equiv f(x_0)\equiv 0 \pmod{p}$．但是，如果$k\neq 0$，则有$x_k-x_0\not\equiv 0 \pmod{p}$，所以对每一个$k\neq 0$，我们必有$g(x_k)\equiv 0 \pmod{p}$，这样，同余式$g(x)\equiv 0 \pmod{p}$对模$p$有$n$个互不同余的解，这与归纳法假设矛盾．证明完成． □

5.6 Lagrange定理的应用

定理5.22 **如果$f(x)=c_0+c_1x+\cdots+c_nx^n$是一个$n$次整系数多项式，并且如果同余式**

$$f(x)\equiv 0 \pmod{p}$$

有多于n个解，其中p是素数．则f的每一个系数都被p整除．

证明　如果有某些系数不被p整除，令c_k是其中足标最大的一个．则$k\leqslant n$并且同余式

$$c_0+c_1x+\cdots+c_kx^k\equiv 0 \pmod{p}$$

有多于p个解．所以，由Lagrange定理，$p|c_k$，这是一个矛盾． □

现在我们应用定理5.22去讨论一个特殊的多项式．

定理5.23　对任一素数p，多项式

$$f(x)=(x-1)(x-2)\cdots(x-p+1)-x^{p-1}+1$$

的所有系数均被p整除.

证明　令$g(x)=(x-1)(x-2)\cdots(x-p+1)$，g的根1，2，…，$p-1$满足同余式

$$g(x)\equiv 0 \pmod{p},$$

根据Euler—Fermat定理，这些数也满足同余式 $h(x)\equiv 0 \pmod{p}$，其中

$$h(x)=x^{p-1}-1.$$

差$f(x)=g(x)-h(x)$为$p-2$次而同余式$f(x)\equiv 0 \pmod{p}$有$p-1$个解，因此，根据定理5.22，$f(x)$的每一个系数都被p整除．　□

由定理5.23里的多项式$f(x)$的两个特殊的系数，我们得到下面两个定理．

定理5.24　Wilson定理．对任意素数p，我们有

$$(p-1)!\equiv -1 \pmod{p}.$$

证明　定理5.23里的多项式$f(x)$的常数项是$(p-1)!+1$．　□

注意，Wilson定理的逆定理也成立．即如果$n>1$且$(n-1)!\equiv -1 \pmod{p}$，则n是素数．（参看习题5.7．）

定理5.25　Wolstenholme定理．对任一素数$p\geq 5$，我们有

$$\sum_{k=1}^{p-1}\frac{(p-1)!}{k}\equiv 0 \pmod{p^2}.$$

证明　定理所讨论的和是数1，2，…，$p-1$中每次取$p-2$个数的所有可能的乘积之和，它也等于多项式

$$g(x)=(x-1)(x-2)\cdots(x-p+1)$$

中$-x$的系数．实际上，$g(x)$能写为形式

$$g(x)=x^{p-1}-s_1x^{p-2}+s_2x^{p-3}-\cdots+s_{p-3}x^2$$
$$-s_{p-2}x+(p-1)!,$$

其中系数s_k是这些根的k个基本对称函数，即1，2，…，$p-1$中每次取k个的所有可能的乘积之和．定理5.23表明，s_1，s_2，…，s_{p-2}的每一个都能被p整除，我们想证明s_{p-2}能被p^2整除．

由$g(x)$的乘积表达式看出$g(p)=(p-1)!$，所以

$$(p-1)!=p^{p-1}-s_1p^{p-2}+\cdots+s_{p-3}p^2-s_{p-2}p$$
$$+(p-1)!.$$

消去$(p-1)!$并对模p^3简化这个等式，因$p\geqslant5$，我们看出

$$pS_{p-2}\equiv0\pmod{p^3}$$

于是$S_{p-2}\equiv0\pmod{p^2}$，符合要求． □

5.7 一次同余式组，中国剩余定理

两个或更多个的一次同余式做成的同余式组不一定有解，甚至即使每一个单个的同余式都有解．例如，没有一个x，它能同时满足$x\equiv1\pmod2$与$x\equiv0\pmod4$，即使这些独立的同余式的每一个有解．在这个例子里，模2与模4是不互素的．下面我们将证明，单独的每个同余式有解的同余式组，如果它们的模是两两互素的，则这个同余式组也有公解．我们从一个特殊的情形着手．

定理5.26 中国剩余定理．设m_1，m_2，…，m_r是两两互素的正整数，即当$i\neq k$时，$(m_i, m_k)=1$．令b_1，…，b_r是任意整数，则同余式组

$$x \equiv b_1 \pmod{m_1}$$

$$\cdots\cdots\cdots\cdots\cdots\cdots$$

$$x \equiv b_r \pmod{m_r}$$

对乘积模$m_1 \cdots m_r$有且仅有一个解.

证明　令$M = m_1 \cdots m_r$并令$M_k = \dfrac{M}{m_k}$，则$(M_k, m_k) = 1$，所以M_k对模m_k有唯一的倒数M_k'，于是令

$$x = b_1 M_1 M_1' + b_2 M_2 M_2' + \cdots + b_r M_r M_r',$$

在这个和里对模m_k讨论每一项，因为，如果$i \neq k$，有$M_i \equiv 0 \pmod{m_k}$，我们有

$$x \equiv b_k M_k M_k' \equiv b_k \pmod{m_k},$$

于是x满足这个同余式组的每一个同余式. 又容易看出这个组对模M只有唯一解. 事实上，如果x与y是这个组的两个解，我们有$x \equiv y \pmod{m_k}$对每个k成立，而m_k是两两互素的，所以有$x \equiv y \pmod{M}$. 证明完成. □

下面的推广容易得到

定理5.27　设m_1，…，m_r是两两互素的，令b_1，…，b_r是任意的整数，a_1，…，a_r满足

$$(a_k, m_k) = 1，对k = 1, 2, \cdots, r.$$

则一次同余式组

$$a_1 x \equiv b_1 \pmod{m_1}$$

$$\cdots\cdots\cdots\cdots\cdots\cdots$$

$$a_r x \equiv b_r \pmod{m_r}$$

对模$m_1 m_2 \cdots m_r$有唯一解.

证明　令a_k'表示a_k对模m_k的倒数，因$(a_k, m_k) = 1$，故a_k'是存在的. 于是同余式$a_k x \equiv b_k \pmod{m_k}$等价于同余式

$x\equiv b_k a_k^{\prime}\ (\mathrm{mod}\, m_k)$. 再利用定理5.26即得结论.

5.8 中国剩余定理的应用

第一个应用是对复合数模的多项式同余式.

定理5.28 **令f是一个整系数多项式，$m_1, m_2, \cdots, m_r$是两两互素的正整数，并令$m=m_1m_2\cdots m_r$. 则同余式**

(12) $f(x)\equiv 0 \quad (\mathrm{mod}\, m)$

有一个解，当且仅当同余式组

(13) $f(x)\equiv 0 \quad (\mathrm{mod}\, m_i) \quad i=1, 2, \cdots, r$

的每一个有一个解. 并且，如果$V(m)$与$V(m_i)$分别表示(12)与(13)的解的个数，则有

(14) $V(m)=V(m_1)V(m_2)\cdots V(m_r)$.

证明　如果$f(a)\equiv 0\ (\mathrm{mod}\, m)$，则$f(a)\equiv 0\ (\mathrm{mod}\, m_i)$对每个$i$成立，于是(12)的每个解也是(13)的解.

反之，令a_i是(13)的一个解，于是根据中国剩余定理，存在一个整数a，使得

(15) $a\equiv a_i \quad (\mathrm{mod}\, m_i) \quad i=1, 2, \cdots, r$,

所以　$f(a)\equiv f(a_i)\equiv 0\ (\mathrm{mod}\, m_i)$.

因为这些模是两两互素的，故我们也有$f(a)\equiv 0\ (\mathrm{mod}\, m)$. 因此，如果(13)的每一个同余式有解，则(12)也有解.

根据定理5.26，我们还知道，同余式组(13)的每一个r一元的解$(a_1, \cdots a_r)$给出满足(15)的唯一整数a mod$m$. 当每个a_i通过(13)的$V(m_i)$个数时，满足(15)也就满足(13)的整数a通过$V(m_1)\cdots V(m_r)$个数. 这证明了(14). □

注意　如果m有素数幂分解式

$$m = p_1^{\alpha_1} \cdots p_r^{\alpha_r},$$

我们可以在定理5.28里取$m_i = p_i^{\alpha_i}$，我们看到，对复合数模同余式的解的问题归结为对素数幂的模．不久，我们将证明，这个问题能进一步归结为素数模的同余式加上一个同余式组．（参看5.9节．）

中国剩余定理的下一个应用涉及由原点可见的格点集合（参看3.8节）

定理5.29　在平面上由原点可见的格点集合包含任意大的方形间断．即，给定任意整数$k>0$，则存在一个格点(a, b)，使得没有任何格点

$$(a+r,\ b+s)\quad 0<r\leqslant k,\ 0<s\leqslant k$$

是由原点可见的．

证明　令$p_1, p_2, \cdots$，是素数序列．已知$k>0$，做$k\times k$阶矩阵，它的第一行由前k个素数组成，第二行由其次的k个素数组成，等等．令m_i是第i行的素数的乘积，M_i是第i列素数的乘积，则m_i是两两互素的，M_i也是两两互素的．下面考虑同余式组

$$x \equiv -1 \pmod{m_1}$$
$$x \equiv -2 \pmod{m_2}$$
$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$
$$x \equiv -k \pmod{m_k},$$

此同余式组对模$m_1 m_2 \cdots m_k$有唯一解a．类似地，同余式组

$$y \equiv -1 \pmod{M_1}$$
$$y \equiv -2 \pmod{M_2}$$
$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

$$y \equiv -k \pmod{M_k}$$

对模$M_1 \cdots M_k = m_1 \cdots m_k$也有唯一解b.

现在我们讨论有相对顶点(a, b)与$(a+k, b+k)$的正方形. 这个正方形内部任一格点有形式

$$(a+r, b+s) \quad 0<r<k, 0<s<k,$$

且$r=k$, $s=k$的点位于这个方形的边界上. 现在我们证明, 这些格点都不是由原点可见的. 事实上,

$$a \equiv -r \pmod{m_r}, \quad b \equiv -s \pmod{M_s},$$

所以在r行s列相交处的元素整除$a+r$与$b+s$, 于是$a+r$与$b+s$不互素, 因此格点$(a+r, b+s)$不是由原点可见的. □

5.9 模是素数方幂的多项式同余式

定理5.28证明了, 多项式同余式$f(x) \equiv 0 \pmod{m}$的求解问题能归结为解同余式组

$$f(x) \equiv 0 \pmod{p_i^{\alpha_i}} \quad i=1, 2, \cdots, r,$$

这里$m = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$. 本节我们证明, 此问题能更进一步地归结为素数模的同余式加上一组一次同余式.

令f是一个整系数多项式, 并设对某个素数p为某个$\alpha \geqslant 2$, 同余式

$$(16) \quad f(x) \equiv 0 \pmod{p^\alpha}$$

有一个解, 比如$x=a$. 这里选择a, 使它位于区间

$$0 \leqslant a < p^\alpha.$$

这个解也满足同余式$f(x) \equiv 0 \pmod{p^\beta}$, $\beta<\alpha$. 特别, a满足同余式

$$(17) \quad f(x) \equiv 0 \pmod{p^{\alpha-1}}.$$

用$p^{\alpha-1}$去除a，有

(18) $a=qp^{\alpha-1}+r \quad 0\leqslant r<p^{\alpha-1}$,

由(18)确定的余数r称为是由a生成的．因为$r\equiv a(\bmod p^{\alpha-1})$，所以r也是(17)的解．换言之，同余式(16)在区间$0\leqslant a<p^{\alpha}$里的任一解a生成同余式(17)在区间$0\leqslant r<p^{\alpha-1}$ 里的一个解r．

现在我们先假定(17)在区间$0\leqslant r<p^{\alpha-1}$ 内有一个解r并问(16)在区间$0\leqslant a<p^{\alpha}$内是否有一个解a生成r．如果有，我们就说r能够由 $p^{\alpha-1}$提高到p^{α}．下面的定理指出，r提高的可能性依赖于模p^{α}上的f(r)与模p上的导数f′(r)．

定理5.30　假设$\alpha\geqslant 2$并令r是同余式

(19) $f(x)\equiv 0 \quad (\bmod p^{\alpha-1})$

在区间$0\leqslant r<p^{\alpha-1}$内的一个解．

(a) 设$f'(r)\not\equiv 0\ (\bmod p)$，则r能以唯一的方式由$p^{\alpha-1}$提高到$p^{\alpha}$，即在区间$0\leqslant a<p^{\alpha}$内有唯一的a生成r，并满足同余式

(20) $f(x)\equiv 0 \quad (\bmod p^{\alpha})$．

(b) 若$f(r)\equiv 0\ (\bmod p)$，则有两种可能．

(b_1) 如果$f(r)\equiv 0\ (\bmod p^{\alpha})$，则r能以p种不同的方式由$p^{\alpha-1}$提高到$p^{\alpha}$．

(b_2) 如果$f(r)\not\equiv 0\ (\bmod p^{\alpha})$，则r不能由$p^{\alpha-1}$ 提高到p^{α}．

证明　如果n是f的次数，我们有等式（泰勒公式）：

(21) $$f(x+h)=f(x)+f'(x)h+\frac{f''(x)}{2!}h^2+\cdots+\frac{f^{(n)}(x)}{n!}h^n$$

对每个x与h都成立．我们注意每个多项式$\frac{f^{(k)}(x)}{k!}$都是整系数．（读者自己验证）在(21)里取$x=r$，这里r是(19)在区间$0\leqslant r<p^{\alpha-1}$内的一个解．又令$h=qp^{\alpha-1}$，这里q是一个整数是指定的．因为$\alpha\geqslant 2$，在(21)里含有$h^2$与h的高次方幂的项都是$p^\alpha$的整数倍．因此，(21)给出同余式

$$f(r+qp^{\alpha-1})\equiv f(r)+f'(r)qp^{\alpha-1}\quad(\mathrm{mod}\,p^\alpha).$$

因为r满足(19)，所以我们可写$f(r)=kp^{\alpha-1}$对某个整数k．最后的同余式变为

$$f(r+qp^{\alpha-1})\equiv\{qf'(r)+k\}p^{\alpha-1}\quad(\mathrm{mod}\,p^\alpha).$$

现在令

(22) $a=r+qp^{\alpha-1}$，

则(a)满足同余式(22)当且仅当q满足一次同余式

(23) $qf'(r)+k\equiv 0\quad(\mathrm{mod}\,p)$．

如果$f'(r)\not\equiv 0\ (\mathrm{mod}\,p)$，则这个同余式对模p有唯一解q，并且如果我们选取q在区间$0\leqslant q<p$内，则由(22)给出的数a将满足(20)且位于区间$0\leqslant a<p^\alpha$．

如果$f'(r)\equiv 0\ (\mathrm{mod}\,p)$，则(23)有解q当且仅当$p|k$，即当且仅当$f(r)\equiv 0\ (\mathrm{mod}\,p^\alpha)$．如果$p\nmid k$，就选不出q去做成a以满足(20)．但若$p|k$，则p个值$q=0,1,\cdots,p-1$给出(20)的p个解a，这些a位于区间$0\leqslant a<p^\alpha$并生成r．证明完成．　□

前述定理的证明也给出了解同余式(20)的一个方法，如果(19)的解是已知的话，反复使用这个可法可把问题最后归结为解同余式

(24) $f(x)\equiv 0\quad(\mathrm{mod}\,p)$．

如果(24)没有解，则(20)也没有解．如果(24)有解，我们选取一个r，位于$0\leqslant r<p$．与r相对应，同余式

$$(25)\quad f(x)\equiv 0 \pmod{p^2}$$

的0，1或p个解．由数$f'(r)$与$k=\frac{f(r)}{p}$确定．如果$p\nmid k$且$p\mid f'(r)$，则r不能提高为(25)的解．这时，我们重新开始讨论另一个解r，如果没有r能提高为(25)的解，则(25)没有解．

如果对于某个r有$p\mid k$，则我们仔细考察同余式

$$qf'(r)+k\equiv 0 \pmod{p},$$

由$p\nmid f'(r)$或$p\mid f'(r)$而确定这个同余式有1个或p个解q．对每个解q，数$a=r+qp$给出(25)的一个解．对于(25)的每一个解都能用类似的步骤去得到

$$f(x)\equiv 0 \pmod{p^3}$$

的所有的解，等等，直至得到(20)的所有的解为止．□

5.10 交叉分类原理

数论中的某些问题能利用关于集合的普通的结合定理来处理，这个定理称为交叉分类原理．（即逐步淘汰原理——译者．）它是一个计算有限集S中不属于某些指定的子集S_1，…，S_n的元素的个数的公式．

注：如果T是S的子集，T的元素的个数记为N(T)，我们用S—T表示S中的不在T里的元素的集合，这样

$$S-\bigcup_{i=1}^{n} S_i$$

由S中的不属于子集合S_1，…，S_n中任何一个的那些元素组

成．为了简便，我们把交集$S_i \cap S_j$，$S_i \cap S_j \cap S_k$，…，分别记为S_iS_j，$S_iS_jS_k$，….

定理5.31　交叉分类原理．如果S_1，…，S_n是有限集S的给定的子集合，则

$$
\begin{aligned}
N(S-\bigcup_{i=1}^{n} S_i)=N(S)-&\sum_{1\leqslant i\leqslant n} N(S_i)\\
&+\sum_{1\leqslant i<j\leqslant n} N(S_iS_j)\\
&-\sum_{1\leqslant i<j<k\leqslant n} N(S_iS_jS_k)+\cdots\\
&+(-1)^n N(S_1S_2\cdots S_n).
\end{aligned}
$$

证明　如果$T\subseteq S$，令$N_r(T)$表示T中不属于前r个子集合S_1，…，S_r中任何一个的元素的个数，$N_0(T)$即$N(T)$．把$N_{r-1}(T)$计算的元素分为两个不相交的集合，一些在S_r中，另一些不在S_r中，因此有

$$N_{r-1}(T)=N_r(T)+N_{r-1}(TS_r),$$

于是有

$$(26)\quad N_r(T)=N_{r-1}(T)-N_{r-1}(TS_r).$$

现在取$T=S$，并利用(26)，用N_{r-2}表示右边的每一项，我们得

$$
\begin{aligned}
N_r(S)=&\{N_{r-2}(S)-N_{r-2}(SS_{r-1})\}\\
&-\{N_{r-2}(S_r)-N_{r-2}(S_rS_{r-1})\}\\
=&N_{r-2}(S)-N_{r-2}(S_{r-1})-N_{r-2}(S_r)\\
&+N_{r-2}(S_rS_{r-1})
\end{aligned}
$$

多次利用(26)，我们得

$$
\begin{aligned}
N_r(S)=N_0(S)-\sum_{i=1}^{r} N_0(S_i)+\sum_{1\leqslant i<j\leqslant r} N_0(S_iS_j)\\
-\cdots+(-1)^r N(S_1\cdots S_r).
\end{aligned}
$$

当$r=n$时，这就给出了所求的公式． □

例 Euler函数的乘积公式能由交叉分类原理得到．令p_1，…，p_r为n的不同素约数．令$S=\{1, 2, \cdots n\}$，并令S_k是S中被p_k整除的那些数组成的S的子集，S中与n互素的那些数不在集合S_1，…，S_r的任何一个中，所以

$$\varphi(n)=N\left(S-\bigcup_{k=1}^{r} S_k\right).$$

如果d/n，则集合S中有$\frac{n}{d}$个数是d的倍数，于是

$$N(S_i)=\frac{n}{p_i},\quad N(S_iS_j)=\frac{n}{p_ip_j},\quad \cdots,$$

$$N(S_1\cdots S_r)=\frac{n}{p_1\cdots p_r},$$

所以由交叉分类原理给出

$$\varphi(n)=n-\sum_{i=1}^{r}\frac{n}{p_i}+\sum_{1\leqslant i<j\leqslant r}\frac{n}{p_ip_j}-\cdots$$

$$+(-1)^r\frac{n}{p_1\cdots p_r}$$

$$=n\sum_{d\mid n}\frac{\mu(d)}{d}=n\prod_{p\mid n}\left(1-\frac{1}{p}\right).$$

交叉分类原理的下一应用是计算模d的一个给定的剩余类r中是模k的一个简化剩余系中的数的个数．这里$d|k$，$(r, d)=1$．

定理5.32 **给定整数r，d与k，$d|k$，$d>0$，$k\geqslant 1$且$(r, d)=1$，则集合**

$$S=\left\{r+td: t=1, 2, \cdots, \frac{k}{d}\right\}$$

中与k互素的元素的个数是$\frac{\varphi(k)}{\varphi(d)}$.

证明　如果素数p整除k与$r+td$，则$p\nmid d$，否则$p|r$与假设$(r, d)=1$矛盾．因此，整除k与S中元素的素数是不能整除d的．记这些素数为p_1，…，p_m，并令

$$k'=p_1\cdots p_m,$$

则S中与k互素的那些数是不能被任何一个这样的素数整除的，令

$$S_i=\{x: x\in S且p_i|x\}\quad i=1, 2, \cdots, m.$$ 如果$x\in S_i$且$x=r+td$，则$r+td\equiv 0 \pmod{p_i}$．因为$p_i\nmid d$，所以存在一个对模p_i唯一的t具有此性质．因此在区间$[1, p_i]$，$[p_i+1, 2p_i]$，…，$[(q-1)p_i+1, qp_i]$的每一个中确有一个t，这里$qp_i=\frac{k}{d}$.

因此

$$N(S_i)=\frac{\frac{k}{d}}{p_i},$$

类似地有

$$N(S_iS_j)=\frac{\frac{k}{d}}{p_ip_j}, \cdots, N(S_1\cdots S_m)=\frac{\frac{k}{d}}{p_1\cdots p_m}.$$

于是，根据交叉分类原理，S中与k互素的整数的个数是

$$N(S-\bigcup_{i=1}^{m}S_i)=\frac{k}{d}\sum_{\delta|k'}\frac{\mu(\delta)}{\delta}=\frac{k}{d}\prod_{p|k'}\left(1-\frac{1}{p}\right)$$

$$=\frac{k\prod\limits_{p|k}\left(1-\frac{1}{p}\right)}{d\prod\limits_{p|d}\left(1-\frac{1}{p}\right)}=\frac{\varphi(k)}{\varphi(d)}.\qquad\Box$$

5.11 简化剩余系的分解性

应用前述定理来讨论简化剩余系的一个性质，此性质在下一章将会用到．首先，我们看一个例子．

令S是模15的一个简化剩余系，如

$$S=\{1, 2, 4, 7, 8, 11, 13, 14\}.$$

我们把S中的 8 个数排为4×2阶矩阵如下：

$$\begin{pmatrix} 1 & 2 \\ 4 & 8 \\ 7 & 11 \\ 13 & 14 \end{pmatrix}.$$

注意，它的每一行都是模 3 的一个简化剩余系，而每一列里的数对模 3 都相互同余．这个例子说明了在下面定理中叙述的简化剩余系的一个性质．

定理5.33 **令S是模k的一个简化剩余系，并令$d>0$是k的一个约数．则我们有下面的S的分解性：**

(a) S是 $\dfrac{\varphi(k)}{\varphi(d)}$ 个不相交的集合的并，而这些集合的每一个都是模d的简化剩余系．

(b) S是$\varphi(d)$个不相交的集合的并，这些集合的每一个由 $\dfrac{\varphi(k)}{\varphi(d)}$ 个对模相互同余的数组成．

注：在前述例子里，$k=15$而$d=3$．矩阵的行表示(a)的不同的集合，列表示(b)的不同集合．如果我们对约数$d=5$应用此定理，我们得到由矩阵

$$\begin{bmatrix} 1 & 2 & 4 & 8 \\ 11 & 7 & 14 & 13 \end{bmatrix}$$

给出的分解，每一行是模 5 的简化剩余系，而每一列由对模 5 相互同余一些数组成．

证明　首先我们证明性质(a)与(b)是等价的．如果(b)成立，我们能把S中的$\varphi(k)$个元素排成一个矩阵，用(b)里的$\varphi(d)$个不相交的集合作矩阵的列，这个矩阵有$\frac{\varphi(k)}{\varphi(d)}$行．每一行就是模d的一个简化剩余系并且它们就是(a)部分要求的不相交的集合．类似地，容易验证(a)可推出(b)．

现在我们证明(b)．令S_d是模d的一个简化剩余系，并设$r\in S_d$．我们证明，在S中至少有$\frac{\varphi(k)}{\varphi(d)}$个对模k不同余的整数n，使得$n\equiv r\pmod d$．因为在$S_d$里，r有$\varphi(d)$个值，而在S里，有$\varphi(k)$个整数，这样的数n不能超过$\frac{\varphi(k)}{\varphi(d)}$个．这证明了(b)．

所需的数n能由模k的剩余类中选出，用下面的$\frac{k}{d}$个整数表示：

$$r,\ r+d,\ r+2d,\ \cdots,\ r+\frac{k}{d}d.$$

这些数对模d是相互同余的，而它们对模k是不同余的．因为$(r,\ d)=1$，由定理5.32说明它们中有$\frac{\varphi(k)}{\varphi(d)}$个与k互素，证明完成．□

第五章习题

1．令S是n个整数（不一定不同）的一个集合，证明S的某个非空子集的元素之和能被n整除．

2．证明　$5n^3+7n^5\equiv 0\pmod{12}$对所有的整数n．

3．(a)找出所有的正整数n，使$n^{13}\equiv n\pmod{1365}$．

(b)找出所有的正整数n使$n^{17}\equiv n\ (\mathrm{mod}\ 4080)$.

4. (a)证明，当$n=4$与$n=p^a$时，$\varphi(n)\equiv 2\ (\mathrm{mod}\ 4)$. 这里p是一个素数，$p\equiv 3\ (\mathrm{mod}\ 4)$.

 (b)找出所有的n，使得$\varphi(n)\equiv 2(\mathrm{mod}\ 4)$.

5. 划分为英吋的码尺，再分为70等分. 证明4个最短的部分中有两个左端点对应于1与19英吋，问另外两个的右端点是什么？

6. 找出所有的x，它同时满足同余式组

$x\equiv 1\ (\mathrm{mod}\ 3)$，$x\equiv 2\ (\mathrm{mod}\ 4)$，$x\equiv 3\ (\mathrm{mod}\ 5)$.

7. 证明 Wilson 定理的逆定理：如果$(n-1)!+1\equiv 0\ (\mathrm{mod}\ n)$，$n>1$，则n是素数.

8. 找出所有的正整数n，使$(n-1)!+1$是n的方幂.

9. 如果p是一个奇素数，令$q=\dfrac{(p-1)}{2}$，证明

$$(q!)^2+(-1)^q\equiv 0\quad(\mathrm{mod}\ p).$$

这就给出q!显然是$x^2+1\equiv 0\ (\mathrm{mod}\ p)$的解，当$p\equiv 1\ (\mathrm{mod}\ 4)$时. 如果$p\equiv 3\ (\mathrm{mod}\ 4)$，则$q!\equiv\pm 1\ (\mathrm{mod}\ p)$. 还没有简单的一般规则去确定这个正负符号.

10. 如果p是奇数，$p>1$，证明

$$1^2 2^2 5^2\cdots(p-2)^2\equiv(-1)^{\frac{(p+1)}{2}}\quad(\mathrm{mod}\ p),$$

且

$$2^2 4^2 6^2\cdots(p-1)^2\equiv(-1)^{\frac{(p+1)}{2}}\quad(\mathrm{mod}\ p).$$

11. 令p是素数，$p\geqslant 5$，并写

$$1+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{p}=\frac{r}{pS},$$

证明 $p^3|(r-S)$.

12. 如果p是素数，证明

$$\binom{n}{p}\equiv\left[\frac{n}{p}\right]\pmod{p},$$

还有，如果 $p^2\left|\left[\frac{n}{p}\right]\right.$，证明，

$$p^2 \mid \binom{n}{p}.$$

13. 令a，b，n都是正整数，使得n整除a^n-b^n，证明n也整除$\frac{(a^n-b^n)}{(a-b)}$.

14. 令a，b与x_0都是正整数并规定

$$x_n=ax_{n-1}+b \quad 对n=1，2，\cdots，$$

证明，所有的x_n都不是素数.

15. 令n，r，a表正整数，同余式$n^2\equiv n(\bmod 10^a)$推出$n^r\equiv n$ $(\bmod 10^a)$对所有的r．找出所有的r，使得$n^r\equiv n$ $(\bmod 10^a)$推出$n^2\equiv n(\bmod 10^a)$.

16. 令n，a，d是给定的整数且$(a，d)=1$，证明，存在一个整数m，使得$m\equiv a(\bmod d)$且$(m，n)=1$.

17. 令f是一个整数值的数论函数，使得

$$f(m+n)\equiv f(n) \pmod{m}$$

对所有的$m\geqslant 1$，$n\geqslant 1$成立．令g(n)是函数值（包括重复）$f(1)，f(2)，\cdots，f(n)$中被n整除的个数，并令h是这些值中与n互素的个数，证明，

$$h(n)=n\sum_{d\mid n}\mu(d)\frac{g(d)}{d}.$$

18. 给定一个奇数$n>3$，令k与t是最小的正整数使$kn+1$与tn二者都是平方数．证明，n是素数当且仅当k与t都

大于$\frac{n}{4}$.

19．证明，$n-1$个连续整数的集合

$$n!+2,\ n!+3,\ \cdots,\ n!+n$$

中的每一个数可被一个素数整除，同时这个素数不能整除这个集合中的其它任何一个数.

20．证明，对任意正整数n与k，存在n个连续整数的集合，使得这个集合中的每一个数能被k个不同的素数整除，而这k个不同的素数没有一个能整除集合中的其它的任何数.

21．令n是一个正整数，它不是一个平方数，证明，对任一与n互素的整数a，存在整数x与y满足

$$ax\equiv y \pmod{n},\quad 0<x<\sqrt{n},\quad 0<|y|<\sqrt{n}.$$

22．令p是素数，$p\equiv 1 \pmod 4$，又令$q=\frac{(p-1)}{2}$，$a=q!$

(a) 证明，存在正整数x与y满足$0<x<\sqrt{p}$与$0<y<\sqrt{p}$，使得

$$a^2x^2-y^2\equiv 0 \pmod{p}.$$

(b) 对于在(a)里的x与y，证明$p=x^2+y^2$．即证明每一素数$p\equiv 1 \pmod 4$是两个平方数之和.

(c) 证明素数$p\equiv 3 \pmod 4$不能是两个平方数之和.

第六章　有限Abel群及其特征

6.1　定义

在第二章里我们提到过群但没有利用它们的性质．现在，我们想更详细地描述群论的一些基本概况．在第七章里，在关于算术级数里的素数的Dirichlet定理的论述中，需要一些被称为Dirichlet特征的数论函数的知识，虽然Dirichlet特征的研究可以在没有任何群论知识的情况下进行，但是，介绍一些最少量的群的知识能使Dirichlet特征的论述处于一种更自然的状态并能简化许多论述．

定义　群的条件，一个群G是元素具有二元运算的一个非空集合，这种运算我们用·表示，它满足下列条件：

(a) 封闭性．对于G中任意的a与b，$a\cdot b$也在G中．

(b) 结合性．对于G中任意的a，b，c，我们有$(a\cdot b)\cdot c=a\cdot(b\cdot c)$．

(c) 恒等元存在．G中有唯一的一个元e，被称为恒等元，它使$a\cdot e=e\cdot a=a$，对G中每一个元a都成立．

(d) 逆元存在．对G中每一个元a，在G中存在唯一的一个元b，使得$a\cdot b=b\cdot a=e$，这个b用a^{-1}表示并称为是a的逆元．

注：通常我们略去这个乘号并把$a\cdot b$写为ab．

定义 Abel群．一个群G称为是Abel群，如果它的每一对元都是可换的，即$ab=ba$对G中所有的a和b都成立．

定义 有限群．一个群如果是有限集合，就称为是有限群．这时，G的元素的个数称为是G的阶，记为$|G|$．

定义 子群．群G的一个非空子集合G′，如果在与G相同的运算下它自身也是一个群，则这个群G′称为是G的一个子群．

6.2 群和子群的例子

例1． 平凡子群．每一个群至少有两个子群，G自身和由单独一个恒等元组成的集合$\{e\}$．

例2． 加法运算下的所有整数．具有运算＋的所有整数的集合是一个Abel群．0是恒等元，n的逆元是$-n$．

例3． 乘法运算下的全体非零复数。所有非零的复数的集合具有通常的复数乘法运算时是一个Abel群，1是它的恒等元，Z的逆元是$\frac{1}{Z}$．绝对值为1的所有复数的集合是它的一个子群．

例4． n次单位根．例2和例3里的群都是无限群．有限群的一个例子是集合$\{1, \varepsilon, \varepsilon^2, \cdots \varepsilon^{n-1}\}$，这里$\varepsilon = e^{\frac{2\pi i}{n}}$，运算·是通常的复数乘法运算．阶数为n的这个群称为是n次单位根群，它是例3里的两个群的子群．

6.3 群的基本性质

下面的n个基本定理对任意的群G都成立．除非特别说

明，不要求G是Abel群，也不要求是有限的.

定理6.1 消去律. 如果G中的元a，b，c满足

$aa=bc$或者$ca=cb$，则$a=b$.

证明 在第一种情形里用c^{-1}右乘等式两边并利用结合律，在第二种情形里左乘以c^{-1}. □

定理6.2 逆元的性质. 在任一群G里我们有

(a) $a^{-1}=e$.

(b) 对G中每一个元a，$(a^{-1})^{-1}=a$.

(c)对G中所有的元a和b，$(ab)^{-1}=b^{-1}a^{-1}$. （注意颠倒顺序）

(d) 对G中所有的元a和b，方程$ax=b$有唯一解$x=a^{-1}b$，方程$ya=b$有唯一解$y=ba^{-1}$.

证明

(a) 因为$ee=ee^{-1}$，消去e便得到$e=e^{-1}$.

(b) 因为$aa^{-1}=e$，并且逆元是唯一的，所以a是a^{-1}的逆元.

(c) 根据结合律，我们有

$$(ab)(b^{-1}a^{-1})=a(bb^{-1})a^{-1}=aea^{-1}=aa^{-1}=e,$$

所以$b^{-1}a^{-1}$是ab的逆元.

(d) 再一次用结合律，我们有

$$a(a^{-1}b)=(aa^{-1})b=b,\ (ba^{-1})a=b(a^{-1}a)=b,$$

由消去律，解是唯一的. □

定义 元素的方幂. 如果$a\in G$，对任意的整数n，我们用下面的关系式来定义a^n：

$$a^0=e,\ a^n=aa^{n-1},\ a^{-n}=(a^{-1})^n,\qquad n>0$$

下面的指数的法则能够用归纳法证明，我们略去这些证明.

定理6.3 **如果$a\in G$，则a的任意两个方幂的运算可交换，并且对所有的整数m和n，我们有**

$$a^m a^n = a^{m+n} = a^n a^m, \quad (a^m)^n = a^{mn} = (a^n)^m.$$

还有，如果a和b可交换，我们有

$$a^n b^n = (ab)^n.$$

定理6.4 **子群的标准．如果G'是群G的一个非空子集，则G'是G的子群当且仅当G'满足群的条件(a)和(d)：**

(a) **封闭性：如果a，$b\in G'$，则$ab\in G'$．**

(d) **逆元的存在性：如果$a\in G'$，则$a^{-1}\in G'$．**

证明　每一个子群必然满足(a)与(d)．反之，如果G'满足(a)与(d)，容易证明G'也满足条件(b)和(c)．因为G中所有的元都满足结合性条件(b)，所以G'中结合性条件(b)成立．为了证明在G'中(c)成立，我们注意，G'至少有一个元素a(因为G'非空)，根据(d)，它的逆元$a^{-1}\in G'$，于是根据(a)，$aa^{-1}\in G'$，即$e\in G'$．

6.4　子群的结构

在给定的群G中总可以任意取出一个元素a来，由a的所有方幂a^n($n=0, \pm1, \pm2, \cdots$)组成一个集合，这个集合显然满足条件(a)和(d)，所以是G的一个子群．它被称为是由a生成的循环子群并记为$\langle a\rangle$．

注意$\langle a\rangle$是一个Abel群，甚至G不是Abel群也如此．如果对某个正整数n，有$a^n=e$，这里n是具有这种性质的最小的数，那么子群$\langle a\rangle$是一个n阶有限群，

$$\langle a\rangle=\{a, a^2, \cdots a^{n-1}, a^n=e\},$$

这里的整数n也称为是元素a的阶．阶为n的一个循环子群的例子是在6.2节里提到的n次单位根群．

下面的定理指出，有限群的任何元素的阶是有限的．

定理6.5　如果G是有限的，并且$a\in G$，则有一个正整数$n\leqslant|G|$，使$a^n=e$．

证明　令$g=1|G|$，元素则G的下面的$g+$中至少有两个元素相等：

$$e,\ a,\ a^2,\ \cdots,\ a^g.$$

假设$a^r=a^s$，其中$0\leqslant s<r\leqslant g$．那么我们有

$$e=a^r(a^s)^{-1}=a^{r-s}.$$

取$n=r-s$，定理得到证明．□

如6.2节所注，每一个群G有两个平凡子群，$\{e\}$和G自身，当G是一个有限Abel群时，在$\{e\}$和G之间有一个构造一组递增子群的简单的方法．将在定理6.8里描述的这个方法以下面的分析为基础．

如果G'是有限群G的一个子群，那么对G的任一元素a，有一个整数n，使$a^n\in G'$．如果a已经在G'中，我们就简单地取$n=1$．如果$a\notin G'$，我们可以取n为a的阶，因为有$a^n=e\in G'$．无论怎样，根据良序原理，一定有一个最小的正整数n，使得$a^n\in G'$，我们称这个整数n为a在G中的指数．

定理6.6　令G'是有限Abel群G的一个子群，且$G'\neq G$．在G中挑选一个元素a，$a\notin G'$，并设h是a在G'中的指数．则乘积的集合

$$G''=\{xa^k:\ x\in G'\text{且}k=0,\ 1,\ 2,\ \cdots,\ h-1\}$$

是G的一个包含G'的子群，而且，G''的阶是G'的h倍．

$|G''|=h|G'|$.

证明　为了证明G''是一个子群，我们利用子群的标准．首先我们检验封闭性．在G''中任取两个元素xa^k和ya^j，这里$x, y\in G'$，$0\leqslant k<h$，$0\leqslant j<h$，因为G是Abel群，所以这两个元素的乘积为

(1)　xya^{k+j}.

由于有$k+j=qh+r$，$0\leqslant r<h$，于是

$$a^{k+j}=a^{qh+r}=a^{qh}\cdot a^r=za^r.$$

其中$a=a^{qh}=(a^h)^q\in G'$，这是因为$a^h\in G'$．因此(1)里的元素为$(xyz)a^r=wa^r$，这里$w\in G'$，$0\leqslant r<h$．这证明了G''满足封闭性条件．

其次我们证明G''中每一个元的逆元也在G''中．在G''中任取一元xa^k．如果$k=0$，则这个元的逆元就是x^{-1}，它是在G''中的．如果$0<k<h$，则这个元的逆元是

ya^{h-k}这里$y=x^{-1}(a^h)^{-1}$

它仍然在G''中．这证明了G''确实是G的一个子群．G''包含G'是显然的．

下面我们确定G''的阶．令$m=|G'|$，当x通过G'的m个元素并且k通过h个整数0，1，2，…$h-1$时，我们得到mh个乘积xa^k．如果我们能够证明所有这些元素是互不相同的，那么G''的阶就是mh．考虑两个这样的乘积xa^k与ya^j，并设

$$xa^k=ya^j,\ 0\leqslant j\leqslant k<h.$$

则$a^{k-j}=x^{-1}y$，$0\leqslant k-j<h$．因为$x^{-1}y\in G'$，所以G'中一有a^{k-j}，所以$k=j$，$x=y$．定证明完成．　□

6.5 有限Aael群的特征

定义 令G是任意一个群．定义在G上的一个复值函数f如果它是积性的，即对任意a，$b\in G$，有

$$f(ab)=f(a)f(b),$$

并且对G中某个c，有$f(c)\neq 0$，那么f就称为是G的一个特征．

理定6.7 如果f是一个具有恒等元e的有限群G的一个特征，则$f(e)=1$并且每一个函数值$f(a)$是一个单位根．特别，如果$a^n=e$，则$f(a)^n=1$．

证明 在G中选取c，使$f(c)\neq 0$，因为$ce=c$，我们有

$$f(c)f(e)=f(c),$$

所以$f(e)=1$．如果$a^n=e$，则$f(a)^n=f(a^n)=f(e)=1$ □

例子．每一个群G至少有一个特征，它就是在G上恒等于1的函数．这个特征称为主特征．下一个定理告诉我们，如果G是Abel群并且有有限阶>1，那么G还有其他的特征．

定理6.8 阶为n的有限Abel群有且仅有n个不同的特征．

证明 在定理6.6里我们学过如何由一个已给的子群$G'\neq G$去构造一个新的包含G'的子群G''，并且G''至少有一个元素不在G'中．我们用符号$<G'; a>$去表示在定理6.6中构造的子群G''，即

$$<G'; a>=\{xa^k : x\in G' \text{并且} 0\leq k<h\},$$

这里h是a在G中的指数．

我们把子群$\{e\}$记作G_1，现在我们从G_1开始，多次这样构造．如果$G_1 \neq G$，我们令a_1是G中与e不同的一个元素并规定$G_2 = < G_1; a_1 >$．如果$G_2 \neq G$，令a_2是G中不属于G_2的一个元素并规定$G_3 = < G_2; a_2 >$．继续这样作下去，可得元素a_1，a_2，$\cdots a_t$的一个有限集合和一个相应的子群G_1，G_2，$\cdots G_t$的集合，使得

$$G_{r+1} = < G_r; a_r >,$$

并且 $G_1 \subset G_2 \subset \cdots \subset G_{t+1} = G.$

因为已给的群G是有限的并且每一个G_{r+1}包含有比它的前一个G_r更多的元素，这个过程在有限步之后必然停止。我们考虑这样的一个子群序列并用归纳法证明这个定理．如果它对于G_r是正确的，证明它对于G_{r+1}也是正确的．

显然，G_1有且仅有一个特征，就是恒等于1的函数。因此，假设G_r的阶为m并且G_r有且仅有m个不同的特征．考虑$G_{r+1} = < G_r, a_r >$并设h是a_r在G_r中的指数，即h是使$a_r^h \in G_r$的最小正整数．我们证明有且仅有h个不同的方法把G_r的每一个特征扩大为G_{r+1}的一个特征，并且G_{r+1}的每一个特征一定是G_r的某个特征的扩大．这就是证明G_{r+1}有且仅有mh个特征，并由于mh是G_{r+1}的阶，这也就是对r用归纳法证明定理．

暂时假设能够把G_r的一个特征f扩大为G_{r+1}的一个特征$\overset{\times}{f}$，由积性要求

$$\overset{\times}{f}(xa_r^k) = \overset{\times}{f}(x)\overset{\times}{f}(a_r)^k.$$

但是$x \in G_r$，所以$\overset{\times}{f}(x) = f(x)$，并由上面的等式得出

$$\overset{\times}{f}(xa_r^k) = f(x)f(a_r)^k.$$

这告诉我们，在$\overset{\times}{f}(a_r)$已知时，$\overset{\times}{f}(xa_r^k)$就确定了．

$\overset{\times}{f}(a_r)$的值能是什么？令$c=a_r^h$，因为$c\in G_r$，我们有$\overset{\times}{f}(c)=f(c)$，并由$\overset{\times}{f}$是积性的，我们还有$\overset{\times}{f}(c)=\overset{\times}{f}(a_r)^h$，于是

$$\overset{\times}{f}(a_r)^h=f(c),$$

所以$\overset{\times}{f}(a_r)$是$f(c)$的一个h次根，因此$\overset{\times}{f}(a_r)$最多只有h种选择.

这些分析告诉我们如何去确定$\overset{\times}{f}$. 如果f是G_r的一个给定的特征，我们就选取$f(c)$的h次根中的一个，这里$c=a_r^h$，并且规定$\overset{\times}{f}(a_r)$就是这个根. 于是我们用等式

$$(2)\quad \overset{\times}{f}(xa_r^k)=f(x)\overset{\times}{f}(a_r)^k$$

来确定G_{r+1}中不属于G_r的哪些元素上的$\overset{\times}{f}$. $\overset{\times}{f}(a_r)$的h种选择全都是不同的，所以这给出了h种不同的方法去确定$\overset{\times}{f}(xa_r^k)$. 现在我们验证确定的函数$\overset{\times}{f}$具有所需的积性. 由(2)我们有

$$\begin{aligned}\overset{\times}{f}(xa_r^k\cdot ya_r^j)&=\overset{\times}{f}(xya_r^{k+j})=f(xy)\overset{\times}{f}(a_r)^{k+j}\\&=f(x)f(y)\overset{\times}{f}(a_r)^k\overset{\times}{f}(a_r)^j\\&=\overset{\times}{f}(xa_r^k)\overset{\times}{f}(ya_r^j),\end{aligned}$$

所以$\overset{\times}{f}$是G_{r+1}的一个特征. 没有两个这样的扩大$\overset{\times}{f}$和$\overset{\times}{g}$在G_{r+1}上是相等的，因为否则，扩大为它们的f和g将会在G_r上相等. 因此G_r的m个特征中的每一个都能以h种不同的方法经过扩大产生为G_{r+1}的特征. 而且，如果φ是G_{r+1}的任一特征，那么，限定它在G_r上，它也是G_r的一个特征. 所以这种方法产生了G_{r+1}的所有特征. 证明完成. □

6.6 特征群

在这一节里，G是一个阶为n的有限Abel群，G的主特

征用f_1表示，其余的用f_2，f_3，$\cdots f_n$表示，称为非主特特征．对G中某个a，它们有性质$f(a)\neq 1$．

定理6.9　如果特征的乘法由关系式

$$(f_i f_j)(a)=f_i(a)f_j(a)$$

确定，这个式子对G中每个a成立，则G的特征的集合形成一个阶为n的有限Abel群，我们用$\widehat{G}$表示这个群．$\widehat{G}$的恒等元是主特征f_1，f_i的逆元是$\frac{1}{f_i}$．

证明　用群的条件去检验．这是一个简单的习题．我们略去这个细节．

注意　对每一个特征f，我们有$|f(a)|=1$，于是倒数$\frac{1}{f(a)}$等于共轭复数$\overline{f(a)}$，用$\overline{f}(a)=\overline{f(a)}$定义的函数$\overline{f}$也是G的一个特征，而且对G中每一个a，我们有

$$\overline{f}(a)=\frac{1}{f(a)}=f(a^{-1}).$$

6.7　特征的正交关系式

令G是一个含有元素a_1，a_2，$\cdots a_n$的n阶Abel群，并令f_1，$f_2\cdots f_n$是G的特征，其中G_1是主特征．（注：我们用$A=A(G)$表示$n\times n$矩阵(a_{ij})，第i行第j列的元素$a_{ij}=f_i(a_j)$．我们将证明这个矩阵A有一个逆矩阵并利用这个事实去推导所说的特征的正交关系式．首先，我们确定A的每一行上的元素的和．）

定理6.10　A的第i行上全部元素的和由

$$\sum_{r=1}^{n}(f_i(a_r)=\begin{cases} n & \text{如果}f_i\text{是主特征}(i=1)\\ 0 & \text{其它}\end{cases}$$

给定.

证明　令S表示所讨论的和. 如果$f_i = f_1$，则和式的每一项为1并且$S = n$. 如果$f_i \neq f_1$，则在G中有一个元素b，$f(b) \neq 1$. 随着a_r通过G的所有元素，乘积ba_r也通过G的所有元素，于是

$$S = \sum_{r=1}^{n} f_i(ba_r) = f_i(b)\sum_{r=1}^{n} f_i(a_r) = f_i(b)S.$$

因此$S(1 - f_i(b)) = 0$，因为$f_i(b) \neq 1$，所以$S = 0$. □

现在我们利用这个定理去证明A有逆矩阵.

定理6.11　令A^*表示矩阵A的转置共轭矩阵，那么我们有

$$AA^* = nI,$$

其中I是$n \times n$单位矩阵，于是$n^{-1}A^*$是A的逆矩阵.

证明　令$B = AA^*$，B的第i行第j列的元素b_{ij}由

$$b_{ij} = \sum_{r=1}^{n} f_i(a_r)\overset{\times}{f}_j(a_r) = \sum_{r=1}^{n} f_i\overset{\times}{f}_j(a_r) = \sum_{r=1}^{n} f_k(a_r)$$

给出，其中，$f_k = f_i\overset{\times}{f}_j = \frac{f_i}{f_j}$. 于是$\frac{f_i}{f_j} = f_1$当且仅当$i = j$.

根据定理6.10我们有

$$b_{ij} = \begin{cases} n & \text{当} i = j \text{时}, \\ 0 & \text{当} i \neq j \text{时}, \end{cases}$$

换言之，$B = nI$ □

下面我们用矩阵与它的逆矩阵可交换这一事实去推导特征的正交关系式.

定理6.12　特征的正交关系式，我们有

$$(3)\quad \sum_{r=1}^{n} \overset{\times}{f}_r(a_i)f_r(a_j) = \begin{cases} n & a_i = a_j, \\ 0 & a_i \neq a_j. \end{cases}$$

证明　$AA^* = nI$即$A^*A = nI$. 但A^*的第i行第j列元素是

(3)式左端的和. 证明完成. □

注: 因为$\overline{f_r(a_i)} = f_r(a_i)^{-1} = f_r(a_i^{-1})$, 所以(3)式中的和的一般项等于$f_r(a_i^{-1})f_r(a_j) = f_r(a_i^{-1}a_j)$, 因此这个正交关系式也可表示如下:

$$\sum_{r=1}^{n} f_r(a_i^{-1}a_j) = \begin{cases} n & a_i = a_j, \\ 0 & a_i \neq a_j. \end{cases}$$

当a_i是恒等元时, 我们得到

定理6.13 A的第j列上全体元素的和为

$$(4) \quad \sum_{r=1}^{n} f_r(a_j) = \begin{cases} n & a_j = e, \\ 0 & \text{其它}. \end{cases}$$

6.8 Dirichlet特征

前面是关于任一有限Abel群的特征的讨论. 现在我们专门研究模为一个固定的正整数k的简化剩余类群. 首先, 我们证明, 如果乘法适合定义, 这些剩余类形成一个群.

我们回忆, 模k的一个简化剩余系是对模k两两互不同余的$\varphi(k)$个整数的集合$\{a_1, a_2, \cdots a_{\varphi(k)}\}$, 其中每一个数都与k互素. 每一个整数a所对应的剩余类$\hat{a}$是与a同余modk的所有整数的集合:

$$\hat{a} = \{x : x \equiv a(\bmod k)\}.$$

剩余类的乘法由式子

$$(5) \quad \hat{a} \cdot \hat{b} = \widehat{ab}$$

确定, 即两个剩余类$\hat{a}$与$\hat{b}$的乘积是乘积ab的剩余类.

定理6.14 具有由(5)式定义乘法的模k的全体简化剩余类的集合是一个阶为$\varphi(k)$的有限Abel群. 其恒等元是剩余

类$\hat{1}$，$\hat{a}$的逆元是剩余类$\hat{b}$，b满足$ab\equiv 1(\mathrm{mod}\,k)$。

证明　剩余类的乘法确定封闭性当然满足．类$\hat{1}$显然是恒等元．如果$(a, k)=1$，则存在唯一的b使$ab\equiv 1(\mathrm{mod}\,k)$，于是$\hat{a}$的逆元是$\hat{b}$．最后显然它是Abel群并且它的阶是$\varphi(k)$． □

定义　Dirichet特征．令G是模k的简化剩余类群．对应于G的每一个特征f，我们如下定义一个数论函数$x=x_f$：

$$x(n)=f\hat{n}\qquad \text{如果}(n, k)=1$$

$$x(n)=0\qquad \text{如果}(n, k)>1,$$

则称函数x为模k的Dirichlet特征，主特征x_1有性质

$$x_1(n)=\begin{cases}1 & (n, k)=1\\ 0 & (n, k)>1.\end{cases}$$

定理6.15　模k有$\varphi(k)$个不同的Dirichlet特征，它们都是完全积性的并以周期k而循环．即我们有

(6)　$x(mn)=x(m)x(n)$　对所有的m，n

与　$x(n+k)=x(n)$　对所有的n。

反之，如果x是完全积性的并以周期k循环，并且，当$(n,k)>1$时，$x(n)=0$，则x一定是模k的一个Dirichlet特征。

证明　模k的简化剩余类群G有$\varphi(k)$个特征f，于是，模k有$\varphi(k)$个特征x_f．当m，n都与k互素时，x_f的积性(6)式随f的积性而得到．如果m或n有一个与k不互素时，则mn也与k不互素，于是(6)式的两边都等于0．周期性由$x_f(n)=x(\hat{n})$得出，由$a\equiv b(\mathrm{mod}\,k)$得出$(a, k)=(b, k)$．

为了证明其逆，我们注意，根据式子

$$f(\hat{n})=x(n)\qquad (n, k)=1$$

定义的群G上的函数f是G的一个特征，所以χ是模k的一个Dirichlet特征． □

例 当$k=1$或$k=2$时，$\varphi(k)=1$，这时唯一的Dirichlet特征是主特征χ_1．对于$k\geq3$，由于$\varphi(k)\geq2$，故至少有两个Dirichlet特征．下面的表格展示了$k=3$，4和5的所有Dirichlet特征．

n	1	2	3
$\chi_1(n)$	1	1	0
$\chi_2(n)$	1	-1	0

$k=3$， $\varphi(k)=2$

n	1	2	3	4
$\chi_1(n)$	1	0	1	0
$\chi_2(n)$	1	0	-1	0

$k=4$， $\varphi(k)=2$

n	1	2	3	4	5
$\chi_1(n)$	1	1	1	1	0
$\chi_2(n)$	1	-1	-1	1	0
$\chi_3(n)$	1	i	$-i$	-1	0
$\chi_4(n)$	1	$-i$	i	-1	0

$k=5$， $\varphi(k)=4$

为了填写这些表格，我们利用了当$(n, k)=1$时$\chi(n)^{\varphi(k)}=1$这个事实，所以$\chi(n)$是$\varphi(k)$次单位根．我们还注意到，如果χ是模k的特征，则共轭复数$\bar{\chi}$也是模k的特征，这些知识对于完成$k=3$，$k=4$的表格是足够的．

当$k=5$时，我们有$\varphi(5)=4$．当$(n, 5)=1$时，$\chi(n)$的可能的值为±1与$\pm i$，而且$\chi(2)\chi(3)=\chi(6)=\chi(1)=1$，所以$\chi(2)$与$\chi(3)$是互为倒数的．又$\chi(4)=\chi(2)^2$．这些知识对于填写$\chi=5$的表格是足够的．在验证的时候，我们能利用定

理6.10与定理6.3，它告诉我们，除了第一行与第一列之外的每一行元素或每一列元素之和是零．下面的表格列出了模6与模7的所有Dirichlet特征．

n	1	2	3	4	5	6
$\chi_1(n)$	1	0	0	0	1	0
$\chi_2(n)$	1	0	0	0	-1	0

$k=6\quad \varphi(k)=2$

n	1	2	3	4	5	6	7
$\chi_1(n)$	1	1	1	1	1	1	0
$\chi_2(n)$	1	1	-1	1	-1	-1	0
$\chi_3(n)$	1	ω^2	ω	$-\omega$	$-\omega^2$	-1	0
$\chi_4(n)$	1	ω^2	$-\omega$	$-\omega$	ω^2	1	0
$\chi_5(n)$	1	$-\omega$	ω^2	ω^2	$-\omega$	1	0
$\chi_6(n)$	1	$-\omega$	$-\omega^2$	ω^2	ω	-1	0

$k=7\qquad \varphi(k)=6\qquad \omega=e^{\frac{\pi i}{3}}$

在算术级数里素数的Dirichlet定理的讨论中，我们将要用到下面的模k的正交关系式．

定理6.16 令$\chi_1\cdots$，$\chi_{\varphi(k)}$表示模k的$\varphi(k)$个Dirichlet特征，设m和n是两个整数，$(n, k)=1$，则我们有

$$\sum_{r=1}^{\varphi(k)}\chi_r(m)\overline{\chi_r}(n)=\begin{cases}\varphi(k) & \text{如果} m\equiv n(\bmod k)\\ 0 & \text{如果} m\not\equiv n(\bmod k).\end{cases}$$

证明 如果$(m,k)=1$，则在定理6.12的正交关系式中取$a_i=\hat{n}$，$a_j=\hat{m}$，并注意$\hat{m}=\hat{n}$当且仅当$m\equiv n(\bmod k)$．如果$(m, k)>1$，则和式的每一项为零并且$m\not\equiv n(\bmod k)$．□

6.9 含有Dirichlet特征的和

这一节讨论在算术级数里素数的Dirichlet定理的证明中出现的一些和式．

第一个定理与模k的一个非主特征χ有关，但若χ是任一周期为k的周期数论函数，并且部分和有界，证明也是正确的．

定理6.17 令χ是模k的任一非主特征，f是对所有$x \geqslant x_0$具有连续的负的导数$f'(x)$的非负函数，则当$y \geqslant x \geqslant x_0$时，我们有

$$(7) \quad \sum_{x<n\leqslant y} \chi(n)f(n) = O(f(x)),$$

此外，如果当$x \to \infty$时，$f(x) \to 0$，则无穷级数

$$\sum_{n=1}^{\infty} \chi(n)f(n)$$

收敛，并且对$x \geqslant x_0$，我们有

$$(8) \quad \sum_{n\leqslant x} \chi(n)f(n) = \sum_{n=1}^{\infty} \chi(n)f(n) + O(f(x)).$$

证明　令$A(x) = \sum_{n\leqslant x} \chi(n)$，因为χ是非主特征，所以我们有

$$A(k) = \sum_{n=1}^{k} \chi(n) = 0.$$

根据周期性，对$n = 2, 3, \cdots$，有$A(nk) = 0$，于是，对所有的x有$|A(x)| < \varphi(k)$．换言之，$A(x) = O(1)$．

现在我们利用Abel等式（定理4.2）把（7）里的和表为积分，

$$\begin{aligned}
&\sum_{x<n\leqslant y} \chi(n)f(n) \\
&= f(y)A(y) - f(x)A(x) - \int_x^y A(x)f'(t)dt \\
&= O(f(y)) + O(f(x)) + O\left(\int_x^y (-f'(t)dt\right) \\
&= O(f(x)).
\end{aligned}$$

这证明了(7)式. 如果当$x\to\infty$时, $f(x)\to 0$, 则(7)式表明级数

$$\sum_{n=1}^{\infty} x(n)f(n)$$

收敛, 这是根据Cauchy收敛准则而得. 为了证明(8), 我们指出

$$\sum_{n=1}^{\infty} x(n)f(n)$$
$$=\sum_{n\leq x} x(n)f(n)+\lim_{y\to\infty}\sum_{x<n\leq y} x(n)f(n),$$

因为(7)式右端的极限是$O(f(x))$, 证明完成. □

现在我们利用定理6.17, 对$x\geqslant 1$, 逐次地取$f(x)=\frac{1}{x}$, $f(x)=\frac{(\log x)}{x}$, $f(x)=\frac{1}{\sqrt{x}}$得到:

定理6.18 如果x是模k的任一非主特征, 并且$x\geqslant 1$, 则我们有

$$(9)\quad \sum_{n\leq x}\frac{x(n)}{n}=\sum_{n=1}^{\infty}\frac{x(n)}{n}+O\left(\frac{1}{x}\right),$$

$$(10)\quad \sum_{x\leq x}\frac{x(n)\log n}{n}=\sum_{n=1}^{\infty}\frac{x(n)\log n}{n}+O\left(\frac{\log x}{x}\right),$$

$$(11)\quad \sum_{n\leq x}\frac{x(n)}{\sqrt{n}}=\sum_{n=1}^{\infty}\frac{x(n)}{\sqrt{n}}+O\left(\frac{1}{\sqrt{x}}\right).$$

6.10 对于实的非主特征x, L(1,x)不等于零.

我们用L(1, x)表示(9)式中级数的和, 即

$$L(1,\ x)=\sum_{n=1}^{\infty}\frac{x(n)}{n}.$$

在Dirichlet定理的证明中, 当x是一个非主特征时, 我们必

须肯定$L(1,\chi)\neq0$，对于实的非主特征，我们能证明这是正确的．首先我们考虑$\chi(n)$的约数和．

定理6.19 **令χ是模k的任意实值特征，并令**

$$A(n)=\sum_{d\mid n}\chi(d),$$

则对所有的n，有$A(n)\geqslant0$，并且，如果n是一个平方数，则$A(n)\geqslant1$．

证明　对素数幂，我们有

$$A(p^a)=\sum_{t=0}^{a}\chi(p^t)=1+\sum_{t=1}^{a}\chi(p)^t.$$

因为χ是实值的，所以$\chi(p)$的仅有可能的值为0，1和-1．如果$\chi(p)=0$，则$A(p^a)=1$；如果$\chi(p)=1$，则$A(p^a)=a+1$；如果$\chi(p)=-1$，则

$$A(p^a)=\begin{cases}0 & a\text{是奇数}\\ 1 & a\text{是偶数}.\end{cases}$$

如果a是偶数，在任何情况下都有$A(p^a)\geqslant1$．于是，如果$n=p_1^{a_1}\cdots p_r^{a_r}$，由于$A$是积性的，故有$A(n)=A(p_1^{a_1})\cdots A(p_r^{a_r})$，其中每个因子$A(p_i^{a_i})\geqslant0$，于是$A(n)\geqslant0$．还有，如果$n$是平方数，则每一个指数$a_i$是偶数，所以每个因子$A(p_i^{a_i})\geqslant1$，于是$A(n)\geqslant1$．定理得证．□

定理6.20 **对于模k的任一实值非主特征，令**

$$A(n)=\sum_{d\mid n}\chi(d),\quad B(n)=\sum_{n\leqslant x}\frac{A(n)}{\sqrt{n}},$$

则我们有

(a) **当$x\to\infty$时，$B(x)\to\infty$．**

(b) **对所有的$x\geqslant1$，$B(x)=2\sqrt{x}L(1,\chi)+O(1)$，因此有$L(1,\chi)\neq0$．**

证明　为了证明(a)，我们利用定理6.19，写

$$B(x) \geq \sum_{\substack{n \leq x \\ n=m^2}} \frac{1}{\sqrt{n}} = \sum_{m \leq \sqrt{x}} \frac{1}{m},$$

当$x \to \infty$时，因为调和级数发散，所以最后的和式趋于∞.

为了证明(b)，我们写

$$B(x) = \sum_{n \leq x} \frac{1}{\sqrt{n}} \sum_{d \mid n} \chi(d) = \sum_{\substack{q, d \\ qd \leq x}} \frac{\chi(d)}{\sqrt{qd}}.$$

现在我们引用定理3.17，它证明了

$$\sum_{\substack{q, d \\ qd \leq x}} f(d)g(q)$$

$$= \sum_{n \leq a} f(n)G\left(\frac{x}{n}\right) + \sum_{n \leq b} g(n)F\left(\frac{x}{n}\right) - F(a)G(b),$$

其中$ab = x$，$F(x) = \sum_{n \leq x} f(n)$并且$G(x) = \sum_{n \leq x} g(n)$，我们取$a = b = \sqrt{x}$，并令$f(n) = \frac{\chi(n)}{\sqrt{n}}$，$g(n) = \frac{1}{\sqrt{n}}$，得到

$$(12)\quad B(x) = \sum_{\substack{q, d \\ qd \leq x}} \frac{\chi(d)}{\sqrt{qd}}$$

$$= \sum_{n \leq \sqrt{x}} \frac{\chi(n)}{\sqrt{n}} + \sum_{n \leq \sqrt{x}} \frac{1}{\sqrt{n}} F\left(\frac{x}{n}\right)$$

$$- F(\sqrt{x})G(\sqrt{x}).$$

根据定理3.2我们有

$$G(x) = \sum_{n \leq x} \frac{1}{\sqrt{n}} = 2\sqrt{x} + A + O\left(\frac{1}{\sqrt{x}}\right),$$

其中A是一个常数．又据定理6.18，(11)式，我们有

$$F(x) = \sum_{n \leq x} \frac{\chi(n)}{\sqrt{n}} = B + O\left(\frac{1}{\sqrt{x}}\right),$$

其中$B = \sum_{n=1}^{\infty} \frac{\chi(n)}{\sqrt{n}}$．因为$F(\sqrt{x})G(\sqrt{x}) = 2Bx^{\frac{1}{4}} + O(1)$，等式(12)给我们

$$B(x)=\sum_{n\leqslant\sqrt{x}}\frac{\chi(n)}{\sqrt{n}}\left\{2\sqrt{\frac{x}{n}}+A+O\left(\sqrt{\frac{n}{x}}\right)\right\}$$

$$+\sum_{n\leqslant\sqrt{x}}\frac{1}{\sqrt{n}}\left\{B+O\left(\sqrt{\frac{n}{x}}\right)\right\}$$

$$-2Bx^{\frac{1}{4}}+O(1)$$

$$=2\sqrt{x}\sum_{n\leqslant\sqrt{x}}\frac{\chi(n)}{n}+A\sum_{n\leqslant\sqrt{x}}\frac{\chi(n)}{\sqrt{n}}$$

$$+O\left(\frac{1}{\sqrt{x}}\sum_{n\leqslant\sqrt{x}}|\chi(n)|\right)$$

$$+B\sum_{n\leqslant\sqrt{x}}\frac{1}{\sqrt{n}}+O\left(\frac{1}{\sqrt{x}}\sum_{n\leqslant\sqrt{x}}1\right)$$

$$-2Bx^{\frac{1}{4}}+O(1)$$

$$=2\sqrt{x}L(1,\chi)+O(1)$$

这证明了(b)，于是由(a)与(b)一起显然得出

$L(1,\chi)\neq0$. □

第六章习题

1. 令G是一个非零复数的n次根的集合，如果G是一个乘法群，证明G是n次单位根做成的群.
2. 令G是一个阶为n、恒等元为e的有限群. 如果a_1，…，a_n是G的n个元（可以相同），证明，有整数p和q，$1\leqslant p\leqslant q\leqslant n$，使$a_pa_{p+1}\cdots a_q=e$.
3. 令G是所有二阶矩阵$\begin{pmatrix}a & b\\ c & d\end{pmatrix}$的集合，其中a，b，c，d是整数，$ad-bc=1$. 证明，G关于矩阵乘法作成一个群，这个群有时称为模群.

4. 令$G=\langle a\rangle$是由a生成的循环群，证明G的每一个子群都是循环群.（没有假设G是有限群）.

5. 令G是一个阶为n的有限群，并令G'是阶为m的一个子群，证明$m|n$（Lagrange定理）. 并推导出，G的每一个元素的阶整除n.

6. 令G是一个阶为6的群，恒等元是e. 证明，或者G是一个循环群，或者G中有两个元素a和b，使得

$$G=\{a,\ a^2,\ a^3,\ b,\ ab,\ a^2b\},$$

其中$a^3=b^2=e$. 这些元素中哪一个是ba？

7. 阶为n的一个有限群$G=\{a_1,\ a_2,\ \cdots,\ a_n\}$的一个群表格是一个n阶矩阵，它的i行j列位置的元素是a_ia_j. 如果$a_ia_j=e$，证明，$a_ja_i=e$. 换言之，恒等元在群表格上的位置是对称的. 进而证明，若n是偶数，则方程$x^2=e$有偶数个解.

8. 7题的推广. 令$f(p)$表示方程$x^p=e$的解的个数，这里p是n的一个素因数，n是G的阶. 证明，$p|f(p)$.（Cauchy定理）. [提示：考虑有序的p维矢量$(a_1,\ \cdots,\ a_p)$的集合S，其中$a_i\in G$，$a_1,\ \cdots a_p=e$. 在S中有n^{p-1}个P维矢量. 两个这样的P维矢量称为等价的，若一个是另一个的循环排列. 证明$f(p)$等价类恰好包含一个元素而其它的类恰好包含p个元素. 用两种方法计算S的元素个数并推出$p[(f(p)]$.

9. 令G是一个n阶有限群，证明，n是奇数当且仅当G的每一个元素是平方形式. 即对G中每一个元a，在G中存在一个元b，使得$a=b^2$.

10. 叙述并证明9题的推广. 其中条件“n是奇数”用“n与

k互素，$k\geqslant 2$”代替.

11. 令G是一个阶为n的有限群，并令S是一个包含有多于$\frac{n}{2}$个元素的G的子集合. 证明，对G中每一个元素g，在S中有元素a与b，使得$ab=g$.

12. 令G是一个群，并令S是有n个不同元素的G的子集合，它具有性质：由$a\in S$推出$a^{-1}\in S$. 考虑形如ab的n^2个乘积（不必不同），这里$a\in S$，$b\in S$. 证明，最多只有$\frac{n(n-1)}{2}$个这样的乘积属于S.

13. 令f_1，…，f_m是阶为m的有限群G的特征，并令a是G的一个阶为n的元素. 定理6.7指出，每一个数$f_r(a)$是一个n次单位根. 证明，每一个n次单位根经常平均地出现在数$f_1(a)$，$f_2(a)$，…，$f_m(a)$之中. [提示：求和

$$\sum_{r=1}^{m}\sum_{k=1}^{n} f_r(a^k)e^{\frac{-2\pi i k}{n}}$$

的值，并以两种方法去确定$e^{\frac{2\pi i}{n}}$出现的次数.]

14. 列表展示模$k=8$，9和10的所有Dirichlet特征的值.

15. 令x是模k的任一非主特征，证明，对所有整数$a<b$，我们有

$$\left|\sum_{n=a}^{b} x(n)\right|\leqslant\frac{1}{2}\varphi(k).$$

16. 如果x是模k的一个实值特征，则对每一个n，有$x(n)=\pm 1$或0. 所以

$$S=\sum_{n=1}^{k} nx(n)$$

是一个整数．本题证明$12S\equiv 0(\bmod k)$．

(a) 如果$(a, k)=1$，证明$ax(a)S\equiv S(\bmod k)$，

(b) 写$k=2^{\alpha}q$，这里q是奇数．证明，有一个整数a，$(a, k)=1$，使得$a\equiv 3(\bmod 2^{\alpha})$且$a\equiv 2(\bmod q)$．最后，利用(a)推出$12S\equiv 0(\bmod k)$．

17. 一个数论函数f称为是周期的modk，如果$k>0$并且当$m\equiv n(\bmod k)$时，$f(m)=f(n)$．整数k称为f的周期．

(a) 如果f是周期函数modk，证明f有一个最小的正的周期k_0，并且$k_0|k$．

(b) 令f是周期函数并且是积性的，k是f的最小的正的周期．证明，如果$(n, k)=1$，则$f(n)=0$．这证明了f是模k的一个Dirichlet特征．

18. (a) 令f是模k的一个Dirichet特征．如果k是无平方因子数，证明k是f的最小正周期．

(b) 举出模k的一个Dirichlet特征的例子，这个k不是f的最小正周期．

第七章　算术级数里素数的Dirichlet定理

7.1　引言

奇数1，3，5，…，$2n+1$，…作成的算术级数里包含有无穷多个素数．我们自然会问，其他的算术级数是否也有此性质．一个首项为h，公差为k的算术级数由所有下面的数组成：

(1)　$kn+h \quad n=0, 1, 2, \cdots$.

如果h与k有一个公约数d，则这个级数的每一项都能被d整除．如果$d>1$，则这个级数里没有一个素数．换言之，算术级数(1)里有无穷多个素数的必要条件是$(h, k)=1$．Dirichlet最先证明了这个条件也是充分的．这就是说，如果$(k, h)=1$，则算术级数(1)里包含有无穷多个素数．这个结果，就是将在本章证明的著名的Dirichlet定理．

我们回忆，Euler用证明对所有素数展开的级数$\sum p^{-1}$发散的方法，证明了无穷多个素数的存在性．Dirichlet想去证明一个相应的结果，即级数(1)里存在无穷多个素数．在1837年发表的一个很好的学术论文里，Dirichlet公布了一个用巧妙的解析方法证明这个定理的计划．这个证明最

近被几位学者所简化. 本章给出的证明是基于Harold N. Shapiro于1950年发表的证明并且涉及的级数是$\sum p^{-1}\log p$而不是级数$\sum p^{-1}$.

首先，我们指出，对某些特殊级数，利用Euclid证明素数的无穷性的方法的一个修改，可以容易地证明Dirichlet定理.

7.2 形如4n－1和4n＋1的素数的Dirichlet定理

定理7.1 有无穷多个形如4n－1的素数.

证明 用反证法. 假设只有限多个这样的素数，并设p是其中最大的. 考虑整数

$$N=2^2\cdot 3\cdot 5\cdot\cdots\cdot(p-1)\cdot p-1,$$

乘积$3\cdot 5\cdot\cdots\cdot P$的因子中包含了所有$\leqslant P$的奇素数. 因为N是4n－1形式的，且$N>p$，所以N不是素数. 但没有$\leqslant p$的素数能除尽N，所以N的所有素因子都大于p. 而N的素因子不能全是4n＋1形式的，因为多个这样形式的数的乘积仍是4n＋1形式. 于是N有素因子为4n－1形式，它又大于p，这与假设矛盾. □

对于形如4n＋1的素数可用另外的方法去证明.

定理7.2 有无穷多个形如4n＋1的素数.

证明 令N是任一大于1的整数. 我们证明，有素数$p>N$，$p\equiv 1\pmod 4$. 令

$$m=(N!)^2+1.$$

注意m是奇数，$m>1$. 令p是m的最小素因数，数2，3，…

N中没有一个能整除m，所以p>N，即我们有

$$(N!)^2\equiv -1\ (\mathrm{mod}\,p).$$

两边自乘$\frac{(p-1)}{2}$次，得

$$(N!)^{p-1}\equiv(-1)^{\frac{(p-1)}{2}}(\mathrm{mod}\,p).$$

根据Fuler-Fermat定理，$(N!)^{p-1}\equiv 1\ (\mathrm{mod}\,p)$，所以

$$(-1)^{\frac{(p-1)}{2}}\equiv 1\ (\mathrm{mod}\,p)$$

于是差$(-1)^{\frac{(p-1)}{2}}-1$是0或-2. 因为它被p整除，所以它不能为-2，只能为0，即

$$(-1)^{\frac{(p-1)}{2}}=1$$

这就是说$\frac{(p-1)}{2}$是偶数，所以$p\equiv 1\ (\mathrm{mod}\,4)$. 换言之，我们证明了，对任意整数$N>1$，有素数$p>N$，$p\equiv 1\ (\mathrm{mod}\,4)$. 因此有无穷多个形如$4n+1$的素数. □

与上面同样简单的理由也可用于对其它特殊的算术级数的讨论，比如$5n-1$，$8n-1$，$8n-3$和$8n+3$等形式（参看Sierpinski[67]）. 但是，对一般形式的级数$kn+h$，还没有发现一个这样简单的方法.

7.3 Dirichlet定理的证明方案

在定理4.10里我们推出渐近公式

$$(2)\quad \sum_{p\leqslant x}\frac{\log p}{p}=\log x+O(1),$$

这里的和式对所有$\leqslant x$的素数p展开，我们将证明，

Dirichlet定理是下面叙述的渐近公式的一个推论.

定理7.3 如果$k>0$，并且$(h, k)=1$，则对所有的$x>1$，我们有

$$(3)\quad \sum_{\substack{p\leqslant x\\ p\equiv h(\mathrm{mod}\,k)}} \frac{\log p}{p}=\frac{1}{\varphi(k)}\log x+O(1).$$

其中和式在满足条件$p\leqslant x$，$p\equiv h(\mathrm{mod}\,k)$的所有素数p上展开.

因为当$x\to\infty$时，$\log x\to\infty$时，由(3)式得出，有无限多个素数$p\equiv h(\mathrm{mod}\,k)$，于是在级数$nk+h$ $n=0, 1, 2, \cdots$里有无穷多个素数.

注意，(3)式右端的主项是与h无关的，因此(3)式不仅推出Dirichlet定理，而且它也证明，在模k的$\varphi(k)$个简化剩余类用每一类的素数贡献出与(α)相同的主项.

定理7.3的证明将通过一系列引理来展现. 在这一节里我们把这些引理集中在一起以展示这个证明的方案. 整个这一章我们采用下面的记号.

正整数k表示一个固定的模，h是一个与k互素的固定的整数，模k的$\varphi(k)$个Dirichlet特征用

$$x_1, x_2, \cdots, x_{\varphi(k)}$$

表示，x_1表示主特征. 对于$x\neq x_1$，我们用$L(1, x)$与$L'(1, x)$表示下面级数的和：

$$L(1, x)=\sum_{n=1}^{\infty}\frac{x(n)}{n},$$

$$L'(1, x)=-\sum_{n=1}^{\infty}\frac{x(n)\log n}{n}.$$

这两个级数的收敛性已在定理6.18中证明过，而且在定理6.20里我们证明了，当x是实值函数时，$L(1, x)\neq 0$，符

号p表示一个素数，$\sum_{p\leq x}$表示对所有素数$p\leq x$展开的和式。

引理7.4 对$x>1$，我们有

$$\sum_{\substack{p\leq x\\ p\equiv h(\bmod k)}}\frac{\log p}{p}=\frac{1}{\varphi(k)}\log x+\frac{1}{\varphi(k)}\sum_{r=2}^{\varphi(k)}\overline{x}_r(h)\sum_{p\leq x}\frac{x_r(p)\log p}{p}+O(1).$$

如果我们能证明，对每一个$x\neq x_1$，有

$$(4)\quad \sum_{p\leq x}\frac{x(p)\log p}{p}=O(1),$$

则显然由引理7.4可推出定理7.3. 下面的引理表明，这个和式可以不对所有素数展开.

引理7.5 对$x>1$与$x\neq x_1$，我们有

$$\sum_{p\leq x}\frac{x(p)\log p}{p}=-L'(1,x)\sum_{n\leq x}\frac{\mu(n)x(n)}{n}+O(1).$$

因此，如果我们证明了

$$(5)\quad \sum_{n\leq x}\frac{\mu(n)x(n)}{n}=O(1),$$

则由引理7.5可推出(4)式。而(5)式可由下面的引理推出。

引理7.6 对$x>1$与$x\neq x_1$，我们有

$$(6)\quad L(1,x)\sum_{n\leq x}\frac{\mu(n)x(n)}{n}=O(1).$$

如果$L(1,x)\neq 0$，我们能在(6)里消去$L(1,x)$而得到(5). 因此，Diricllet定理的证明最终有赖于对所有

$x \neq x_1$，$L(1, x) \neq 0$．在定理6.20里我们已经证过，对于实值的$x \neq x_1$，有$L(1, x) \neq 0$，因此，余下的问题是证明，对所有复值的$x \neq x_1$，同样有$L(1, x) \neq 0$．

为了这个目的，我们令$N(k)$表示模k的满足$L(1, x)=0$的非主特征x的个数．如果$L(1, x)=0$，则$L(1, \overline{x})=0$并因x不是实的，所以$x \neq \overline{x}$．因此，使$L(1, x)=0$的x成共轭对出现，所以$N(k)$是偶数．我们的目的是证明$N(k)=0$，这能由下面的渐近公式推出．

引理7.7 对$x>1$，我们有

$$(7) \qquad \sum_{\substack{p \leqslant x \\ p \equiv 1 (\mathrm{mod}\, k)}} \frac{\log p}{p} = \frac{1-N(k)}{\varphi(k)} \log x + O(1).$$

如果$N(k) \neq 0$，由于$N(k)$是偶数，所以$N(k) \geqslant 2$，于是(7)里$\log x$的系数是负数并且当$x \to \infty$时，右端$\to -\infty$，而左边所有的项都是正的，这是一个矛盾。因此由引理7.7推出$N(k)=0$．引理7.7的证明以下面的渐近公式为基础．

引理7.8 如果$\chi \neq \chi_1$并且$L(1, \chi)=0$，则我们有

$$L'(1, \chi) \sum_{n \leqslant x} \frac{\mu(n)\chi(n)}{n} = \log x + O(1).$$

7.4 引理7.4的证明

为证明引理7.4，我们从前面提到的渐近公式着手．

$$(2) \qquad \sum_{p \leqslant x} \frac{\log p}{p} = \log x + O(1).$$

在和式中取出由素数$p \equiv h (\mathrm{mod}\, k)$所产生的项。取出的完成是借助于在定理6.16里所表述的Dirichlet正交关系式：

$$\sum_{r=1}^{\varphi(k)} \chi_r(m)\overline{\chi}_r(m)=\begin{cases}\varphi(k) & 如果 m\equiv n(\mathrm{mod}\,k)\\ 0 & 如果 m\not\equiv n(\mathrm{mod}\,k).\end{cases}$$

对于$(n,k)=1$，这是正确的。我们取$m=p$，$n=h$，这里，$(h,k)=1$．将上式两端乘以$p^{-1}\log p$并对所有$\leqslant x$的p求和，我们得到

$$(8)\quad \sum_{p\leqslant x}\sum_{r=1}^{\varphi(k)} \chi_r(p)\overline{\chi}_r(h)\frac{\log p}{p}$$

$$=\varphi(k)\sum_{\substack{p\leqslant x\\ p\equiv h(\mathrm{mod}\,k)}}\frac{\log p}{p}.$$

在左边的和式里我们分离出只含主特征χ_1的这些项，(8)式改写为

$$(9)\quad \varphi(k)\sum_{\substack{p\leqslant x\\ p\equiv h(\mathrm{mod}\,k)}}\frac{\log p}{p}=\overline{\chi}_1(h)\sum_{p\leqslant x}\frac{\chi_1(p)\log p}{p}$$

$$+\sum_{r=2}^{\varphi(k)}\overline{\chi}_r(h)\sum_{p\leqslant x}\frac{\chi_r(p)\log p}{p}.$$

于是$\overline{\chi}_1(h)=1$且当$(p,x)\neq 1$时$\chi_1(p)=0$，当$(p,k)=1$时，$\chi_1(p)=1$．因为只有有限多个素数整除k，于是(9)式右端第一项为

$$(10)\quad \sum_{\substack{p\leqslant x\\ (p,x)=1}}\frac{\log p}{p}=\sum_{p\leqslant x}\frac{\log p}{p}-\sum_{\substack{p\leqslant x\\ p\mid k}}\frac{\log p}{p}$$

$$=\sum_{p\leqslant x}\frac{\log p}{p}+O(1).$$

由(9)与(10)我们得到

$$\varphi(k)\sum_{\substack{p\leqslant x\\ p\equiv h(\mathrm{mod}\,k)}}\frac{\log p}{p}=\sum_{p\leqslant x}\frac{\log p}{p}$$

$$+\sum_{r=2}^{\varphi(k)}\overline{\chi}_r(h)\sum_{p\leqslant x}\frac{\chi_r(p)\log p}{p}+O(1).$$

利用(2)式并除以$\varphi(k)$，我们得到引理7.4 □

7.5 引理7.5的证明

我们从和式

$$\sum_{n\le x}\frac{\chi(n)\Lambda(n)}{n}$$

着手，其中$\Lambda(n)$是Mangoldt函数，用两种方法表示这个和。首先我们注意，由$\Lambda(n)$的定义给我们

$$\sum_{n\le x}\frac{\chi(n)\Lambda(n)}{n}=\sum_{\substack{p\le x\\ p^{\alpha}\le x}}\sum_{\alpha=1}^{\infty}\frac{\chi(p^{\alpha})\log p}{p^{\alpha}}$$

我们分出$\alpha=1$这一项，有

$$(11)\quad \sum_{n\le x}\frac{\chi(n)\Lambda(n)}{n}=\sum_{p\le x}\frac{\chi(p)\log p}{p}+\sum_{\substack{p\le x\\ p^{\alpha}\le x}}\sum_{\alpha=2}^{\infty}\frac{\chi(p^{\alpha})\log p}{p^{\alpha}}$$

右端的第二个和式是主要的，根据

$$\sum_{p}\log p\sum_{\alpha=2}^{\infty}\frac{1}{p^{\alpha}}=\sum_{p}\frac{\log p}{p(p-1)}<\sum_{n=2}^{\infty}\frac{\log n}{n(n-1)}=O(1),$$

所以(11)给我们

$$(12)\quad \sum_{p\le x}\frac{\chi(p)\log p}{p}=\sum_{n\le x}\frac{\chi(n)\Lambda(n)}{n}+O(1).$$

现在我们回忆到$\Lambda(n)=\sum_{d|n}\mu(d)\log\left(\frac{n}{d}\right)$，于是

$$\sum_{n\le x}\frac{\chi(n)\Lambda(n)}{n}=\sum_{n\le x}\frac{\chi(n)}{n}\sum_{d|n}\mu(d)\log\frac{n}{d}.$$

在最后的和式里，我们写$n=cd$并利用χ的积性得到

$$(13)\quad \sum_{n\leqslant x}\frac{\chi(n)\Lambda(n)}{n}=\sum_{d\leqslant x}\frac{\mu(d)\chi(d)}{d}$$

$$\sum_{c\leqslant \frac{x}{d}}\frac{\chi(c)\log c}{c}.$$

因为$\frac{x}{d}\geqslant 1$，在对C求和的式子里我们利用定理6.18的(10)式得到

$$\sum_{c\leqslant \frac{x}{d}}\frac{\chi(c)\log c}{c}=-L'(1,\chi)+O\left(\frac{\log\frac{x}{d}}{\frac{x}{d}}\right),$$

于是等式(13)变为

$$(14)\quad \sum_{n\leqslant x}\frac{\chi(n)\Lambda(n)}{n}=-L'(1,\chi)\sum_{d\leqslant x}\frac{\mu(d)\chi(d)}{d}$$

$$+O\left(\sum_{d\leqslant x}\frac{1}{d}\frac{\log\frac{x}{d}}{\frac{x}{d}}\right).$$

在O一项里和式为

$$\frac{1}{x}\sum_{d\leqslant x}(\log x-\log d)=\frac{1}{x}\left([x]\log x-\sum_{d\leqslant x}\log d\right)$$
$$=O(1),$$

这是因为

$$\sum_{d\leqslant x}\log d=\log[x]!\ =x\log x+O(x).$$

因此(14)变为

$$\sum_{n\leqslant x}\frac{\chi(n)\Lambda(n)}{n}=-L'(1,\chi)\sum_{d\leqslant x}\frac{\mu(d)\chi(d)}{d}$$

$$+O(1).$$

此式与(12)式一起，就证明了引理7.5． □

7.6 引理7.6的证明

我们利用在定理2.23里证明过的Möbius反转公式，它指出，如果α是完全积性函数，我们有

$$(15)\quad G(\chi)=\sum_{n\leqslant \chi}\alpha(n)F\left(\frac{x}{n}\right)\text{当且仅当}F(\chi)$$

$$=\sum_{n\leqslant x}\mu(n)\alpha(n)G\left(\frac{\chi}{n}\right).$$

我们取$\alpha(n)=\chi(n)$，$F(x)=x$，得

$$(16)\quad \chi=\sum_{n\leqslant x}\mu\chi(n)(n)G\left(\frac{x}{n}\right),$$

其中

$$G(x)=\sum_{n\leqslant x}\chi(n)\frac{x}{n}=x\sum_{n\leqslant x}\frac{\chi(n)}{n}.$$

根据定理6.18中的等式(9)，我们可写$G(\chi)=\chi L(1,x)+O(1)$．在(16)式中利用此式，得

$$\chi=\sum_{n\leqslant x}\mu(n)\chi(n)\left\{\frac{x}{n}L(1,x)+O(1)\right\}$$

$$=xL(1,x)\sum_{n\leqslant x}\frac{\mu(n)x(n)}{n}+O(x).$$

用x去除此式即得引理7.6． □

7.7 引理7.8的证明

我们先证明引理7.8然后利用它去证明引理7.7。我们再一次利用Möbius反转公式(15)。这次我们取$F(x)=x\log x$，

得

$$(17)\quad x\log x=\sum_{n\leqslant x}\mu(n)\chi(n)G\left(\frac{x}{n}\right)$$

其中

$$G(x)=\sum_{n\leqslant x}\chi(n)\frac{x}{n}\log\frac{x}{n}=x\log x\sum_{n\leqslant x}\frac{\chi(n)}{n}$$
$$-x\sum_{n\leqslant x}\frac{\chi(n)\log n}{n}.$$

现在我们利用定理6.18中的公式(9)与(10)，得

$$G(x)=x\log x\left\{L(1,\chi)+O\left(\frac{1}{x}\right)\right\}$$
$$+x\left\{L'(1,\chi)+O\left(\frac{\log x}{x}\right)\right\},$$
$$=xL'(1,\chi)+O(\log x)$$

因为我们有假设$L(1,x)=0$. 于是(17)式给出

$$x\log x=\sum_{n\leqslant x}\mu(n)x(n)\left\{\frac{x}{n}L'(1,\chi)\right.$$
$$\left.+O\left(\log\frac{x}{n}\right)\right\}=xL'(1,\chi)\sum_{n\leqslant x}\frac{\mu(n)\chi(n)}{n}$$
$$+O\left(\sum_{n\leqslant x}(\log x-\log n)\right).$$

我们已经知道右端的 O一项是$O(x)$(参看引理7.5的证明)，于是我们有

$$x\log x=xL'(1,\chi)\sum_{n\leqslant x}\frac{\mu(n)\chi(n)}{n}+O(x)$$

当我们用x去除时，即得引理7.8 □

7.8 引理7.7的证明

我们利用引理7.4，当$h=1$时，得

$$(18)\quad \sum_{\substack{p\leqslant x\\ p\equiv 1(\bmod k)}}\frac{\log p}{p}=\frac{1}{\varphi(k)}\log x$$

$$+\frac{1}{\varphi(k)}\sum_{r=2}^{\varphi(k)}\sum_{p\leqslant x}\frac{\chi_r(p)\log p}{p}+O(1),$$

在右端对p求和的式子里，我们引理7.5，即

$$\sum_{p\leqslant x}\frac{\chi_r(p)\log p}{p}=-L'(1,x_r)\sum_{n\leqslant x}\frac{\mu(n)x_r(n)}{n}$$

$$+O(1).$$

如果$L(1,x_r)\neq 0$，由引理7.6说明(18)右端是$0(1)$，而如果$L(1,x_r)=0$，则由引理7.8得

$$-L'(1,x_r)\sum_{n\leqslant x}\frac{\mu(n)\chi_r(n)}{n}=-\log x+0(1),$$

因此(18)右端的和为

$$\frac{1}{\varphi(x)}\Big\{-N(k)\log x+0(1)\Big\},$$

所以(18)式变为

$$\sum_{\substack{n\leqslant x\\ p\equiv 1(\bmod k)}}\frac{\log p}{p}=\frac{1-N(k)}{\varphi(k)}\log x+0(1).$$

这就证明了引理7.7，也证明了定理7.3． □

如前所述，定理7.3可推出Dirichlet定理：

定理7.9　如果$k>0$且$(h,k)=1$，则在算术级数$nk+h$，($n=0,1,2,\cdots$)中有无穷多个素数．

7.9　算术级数里素数的分布

如果$k>0$并且$(a,k)=1$，令

$$\pi_a(x)=\sum_{\substack{p\leqslant x\\ p\equiv a(\bmod k)}}1.$$

则函数$\pi_a(x)$是级数$nk+a$（$n=0, 1, 2, \cdots$）中$\leqslant x$的素数的个数。Dirichlet证明了，当$x\to\infty$时，$\pi_a(x)\to\infty$。算术级数里素数定理也可表述为

$$(19)\quad \pi_a(x)\sim\frac{\pi(x)}{\varphi(k)}\sim\frac{1}{\varphi(k)}\frac{x}{\log x}$$

当$X\to\infty$时，

如果$(a,k)=1$的话．(19)的证明是[44]里的重点．级数的素数定理是由定理7.3的公式提出来的，

$$\sum_{\substack{p\leqslant x\\ p\equiv h\ (\mathrm{mod}\ k)}}\frac{\log p}{p}=\frac{1}{\varphi(k)}\log x+O(1).$$

因为主项与h无关，这些素数好象平均地分布在模k的$\varphi(k)$个简化剩余类里，而(19)式则是这个事实的准确的表述．

我们给出算术级数的素数定理的一个代替形式来结束这一章．

定理7.10　如果

$$(20)\quad \pi_a(x)\sim\frac{\pi(x)}{\varphi(k)}\qquad x\to\infty$$

对每一个与k互素的整数a成立，则有

$$(21)\quad \pi_a(x)\sim\pi_b(x)\qquad \text{当}x\to\infty\text{时},$$

其中$(a,k)=(b,k)=1$．反之，由(21)也可推出(20)．

证明　由(20)推出(21)是显然的．为了证明其逆，我们假定(21)成立，并令$A(k)$表示整除k的素数的个数，如果$x>k$，我们有

$$\pi(x)=\sum_{p\leqslant x}1=A(k)+\sum_{\substack{p\leqslant x\\ p\nmid k}}1$$

$$=A(k)+\sum_{\substack{a=1\\ (a,k)=1}}^{k}\ \sum_{\substack{p\leqslant x\\ p\equiv a\ (\mathrm{mod}\ k)}}1$$

$$=A(k)+\sum_{\substack{a=1\\(a,k)=1}}^{k}\pi_a(x)$$

因此

$$\frac{\pi(x)-A(k)}{\pi_b(x)}=\sum_{\substack{a=1\\(a,k)=1}}^{k}\frac{\pi_a(x)}{\pi_b(x)}.$$

根据(21)式，在$x\to\infty$时，和式里的每一项趋于1，所以这个和式趋于$\varphi(k)$，于是

$$\frac{\pi_a(x)}{\pi_b(x)}-\frac{A(k)}{\pi_b(x)}\to\varphi(k)\quad 当\ x\to\infty时.$$

然而$\frac{A(x)}{\pi_b(x)}\to 0$，所以$\frac{\pi(x)}{\pi_b(x)}\to\varphi(k)$. 这证明(20)成立.

第七章习题

在1至4题里，h与k是已知的正整数，$(h,k)=1$. $A(h,k)$是算术级数，$A(h,k)=\{h+kx:x=0,1,2,\cdots\}$.

解1至4题时不用Dirichlet定理.

1. 证明，对每一个整数$n\geqslant 1$，$A(h,k)$中包含有无穷多个与n互素的数.
2. 证明，$A(h,k)$包含有一个无穷子集合$\{a_1, a_2, \cdots\}$，使得$(a_i, a_j)=1$，当$i\neq j$时.
3. 证明，$A(h,k)$包含有一个无穷子集合，它成为一个几何级数（形如ar^n，$n=0, 1, 2, \cdots$的数集）. 这说明，$A(h,k)$包含有无穷多个具有相同素因子的数.
4. 设S是$A(h,k)$的任一无穷子集合，证明，对每一个正整

数n，在$A(h,k)$中有一个数，它能表示为S中的几个以上不同的数之积.

5. 由Dirichlet定理可推出下面的论断：如果h与$k>0$是任意两个整数，$(h,k)=1$，则至少存在一个形如$kn+h$的素数. 证明，由这个论断也可推出Dirichlet定理.

6. 如果$(h,k)=1$，$k>0$，证明，有一个常数A(依赖于h和k)，使得，当$x\geqslant 2$时，

$$\sum_{\substack{p\leqslant x\\ p\equiv h\,(\bmod k)}}\frac{1}{p}=\frac{1}{\varphi(k)}\log\log x+A+O\left(\frac{1}{\log x}\right).$$

7. 作一个素数的无穷集合S，使它具有如下性质：如果$p\in s$，$q\in s$，则有$\left(\frac{1}{2}(p-1),\frac{1}{2}(q-1)\right)=(p,q-1)=(p-1,q)=1$，

8. 令f是一个次数为$n>1$的整系数多项式，它有下面的性质：对每一个素数p，存在一个素数q和整数m，使得$f(p)=q^m$. 证明，$q=p$，$m=n$，而$f(x)=x^n$对所有x成立. [提示：如果$q\neq p$，则对每一个$t=1,2,\cdots$，都有q^{m+1}整除$f(p+tq^{m+1})-f(p)$.]

第八章　周期数论函数与Gauss和

8.1　模k的周数函数

令k是一个正整数。一个数论函数f称为是一个具有周期k（或周期modk）的周期函数，如果

$$f(n+k)=f(n)$$

对所有整数n成立．如果k是一个周期，则对任意的整数$m>0$，mk也是周期．f的最小的正的周期称为基本周期。

周期函数在前面几章里已经见过．例如模k的Dirichlet特征是周期函数．一个简单的例子是，把最大公约数(n,k)看作是n的函数，由关系式

$$(n+k,\ k)=(n,\ k)$$

得到周期性．另一个例子是指数函数

$$f(n)=e^{\frac{2\pi imn}{k}}$$

其中m和k是固定的整数，$e^{\frac{2\pi im}{k}}$是k次单位根，而f(n)是它的n次方幂．这样一些函数的任意有限个的线性组合，如

$$\sum_{m}c(m)e^{\frac{2\pi imn}{k}}$$

对系数c(m)的每一个选择都是周期函数mod k. 我们的首要目的是证明每一个具有周期k的数论函数都能表示为这种类型的线性组合. 这些和称为有限Fourier级数. 我们从一个简单而重要的例子即著名的几何和开始讨论.

定理8.1 对于固定的$k\geqslant1$，令

$$g(n)=\sum_{m=0}^{k-1}e^{\frac{2\pi imn}{k}},$$

则

$$g(n)=\begin{cases}0 & \text{如果} k\nmid n,\\ k & \text{如果} k\mid n.\end{cases}$$

证明　因为g(n)是几何级数的一些项的和.

$$g(n)=\sum_{m=0}^{k-1}x^m,$$

其中$x=e^{\frac{2\pi in}{k}}$，所以我们有

$$g(n)=\begin{cases}\dfrac{x^k-1}{x-1} & \text{如果} k\nmid n,\\ k & \text{如果} k\mid n.\end{cases}$$

但$x^k=1$，并且$x=1$当且仅当$k\mid n$，所以定理得证. □

8.2 周期数论函数的有限Fourier级数的存在性

我们将利用lagrange的多项式插值公式去证明，每一个周期数论函数有一个有限Fourier展式.

定理8.2 lagrange插值定理. 令z_0，z_1，$\cdots z_{k-1}$是k个不同的复数，W_0，W_1，$\cdots$，W_{k-1}是k个复数，不要求它

们不同，则有唯一的一个次数$\leqslant k-1$的多项式$P(z)$，使得

$$P(z_m)=w_m \qquad m=0,1,2,\cdots k-1$$

证明　所求的多项式$p(z)$叫做lagrange插值多项式，它能直接如下做成．令

$$A(z)=(z-z_0)(z-z_1)\cdots(z-z_{k-1}),$$

并令

$$A_m(z)=\frac{A(z)}{z-z_m},$$

那么$A_m(z)$是一个具有下面性质的次数为$k-1$的多项式：

$$A_m(z_m)\neq 0,\quad A_m(z_j)=0\quad \text{如果} j\neq m.$$

于是$\frac{A_m(z)}{A_m(z_m)}$是一个次数为$k-1$的多项式，对每一个z_j，$j\neq m$，它的值为零；对z_m，它的值为1．因此，线性组合

$$P(z)=\sum_{m=0}^{k-1}W_m\frac{A_m(z)}{A_m(z_m)}.$$

是一个次数$\leqslant k-1$的多项式，对每一个j，有$P(z_j)=W_j$．如果有另一个这样的多项式$Q(z)$满足条件，那么在k个不同的点上差$P(z)-Q(z)$恒为零，而两个多项式的次数都$\leqslant k-1$，所以$P(z)=Q(z)$．

现在我们选取数z_0，z_1，$\cdots z_{k-1}$为k次单位根，得

定理8.3　**给定k个复数w_0，w_1，$\cdots w_{k-1}$，则存在k个唯一确定的复数a_0，a_1，$\cdots a_{k-1}$，使得**

$$(1)\quad W_m=\sum_{n=0}^{k-1}a_ne^{\frac{2\pi imn}{k}}$$

对$m=0,1,2,\cdots,k-1$都成立。此外，系数a_n由公式

$$(2)\quad a_n=\frac{1}{k}\sum_{m=0}^{k-1}W_ne^{\frac{-2\pi imn}{k}}\quad n=0,1,2,\cdots,k-1$$

确定．

证明　令$z_m=e^{\frac{2\pi i m}{k}}$. 由于$z_0$, z_1, …, z_{k-1}是互不相同的，所以有一个唯一的lagrange多项式

$$P(z)=\sum_{n=0}^{k-1}a_n z^n,$$

使得$P(z_m)=W_m$，对每一个$m=0$, 1, 2, …, $k-1$ 成立. 这说明有唯一确定的一组数a_n满足(1). 为了得出a_n的公式(2),我们用$e^{\frac{-2\pi i m r}{k}}$乘(1)的两边，其中m和r是小于k的非负整数，并对m求和，得

$$\sum_{m=0}^{k-1} W_m e^{\frac{-2\pi i m r}{k}}=\sum_{n=0}^{k-1}a_n\sum_{m=0}^{k-1}e^{\frac{2\pi i(n-r)m}{k}},$$

根据定理8.1，m上的这个和是零，除非$k|(n-r)$. 但是$|n-r|\leqslant k-1$，所以$k|(n-r)$当且仅当$n=r$. 因此，右端的仅有的非零的项出现在$n=r$时，我们得到

$$\sum_{m=0}^{k-1} W_m e^{\frac{-2\pi i m r}{k}}=k a_r$$

这个等式给出了我们的(2)式. □

定理8.4　令f是一个具有周期k的数论函数，于是有一个唯一确定的周期也是k的数论函数g，使得

$$f(m)=\sum_{n=0}^{k-1} g(n)e^{\frac{2\pi i m n}{k}}.$$

实际上，g由公式

$$g(n)=\frac{1}{k}\sum_{m=0}^{k-1} f(m)e^{\frac{-2\pi i m n}{k}}$$

给定.

证明　令$W_m=f(m)$, $m=0$, 1, 2, …$k-1$. 利用定理8.3去确定a_0, a_1, …a_{k-1}. 由关系式$g(m)=a_m$, $m=0$, 1, 2, …$k-1$定义函数g，并把g(m)的定义推广到所有的整

数，使其有周期k．于是f与g有定理里的关系式． □

注：因为f和g都是模k的周期函数，我们能把定理8.4里的和式改写 如下：

$$(3)\quad f(m)=\sum_{n \bmod k} g(n)e^{\frac{2\pi imn}{k}},$$

$$(4)\quad g(n)=\frac{1}{k}\sum_{m \bmod k} f(m)e^{\frac{-2\pi imn}{k}}.$$

此二式的求和都在模k的任一完全剩余系上展开．（3）式中的和称为f的有限Fourier展式而由（4）式确定的数$g(n)$称为f的Fourier系数．

8.3 Ramanujan和及其推广

在习题2.14(b)里证明过Möbius函数$\mu(k)$是k次本原单位根的和。本节推广这个结果．特别地，令n是一个固定的正整数并考虑k次本原单位根的n次幂的和．它就是著名的Ramanjuan和并用$C_k(n)$表示：

$$C_k(n)=\sum_{\substack{m \bmod k \\ (m,k)=1}} e^{\frac{2\pi imn}{k}},$$

我们已经注意到，当$n=1$时，这个和简化为Möbius函数

$$\mu(k)=C_k(1).$$

当$\frac{k}{n}$时，这个和简化为Euler函数φ，因为每项是1并且项数是$\varphi(k)$．Ramanujan证明，$C_k(n)$始终是一个整数并具有有趣的乘法性质．由关系式

$$(5)\quad C_k(n)=\sum_{d\mid(n,k)} d\,\mu\left(\frac{k}{d}\right),$$

他推导出了这些性质．

这个公式说明$C_k(m)$能简化为$\mu(k)$与$\varphi(k)$的原因．事

实上，当$n=1$时，这个和只有一项，我们得到$C_k(1)=\mu(k)$．当$\frac{k}{n}$时，我们有$(n,k)=k$并$C_k(n)=\sum_{d|k} d\mu\left(\frac{k}{d}\right)=\varphi(k)$．我们将推出以(5)为特殊形式的更一般的结果（定理8.5）．

$C_k(n)$的公式(5)提示我们研究这种形式的更一般的和

$$(6)\quad \sum_{d|(n,k)} f(d)g\left(\frac{k}{d}\right).$$

这类似于Dirichlet乘积$f*g$的和式，不同之处在于，这里是$d|(n,k)$，而在$f*g$里是$d|n$.

(6)里的和用$S_k(n)$表示．因为n只出现在$\gcd(n,k)$里，而$(n+k,k)=(n,k)$，所以我们有

$$S_k(n+k)=S_k(n),$$

故$S_k(n)$是周期为k的周期函数．于是这个和有一个有限Fourier展式。下面的定理告诉我们，它的Fourier系数由同一类型的和式给出．

定理8.5 **令$S_k(n)=\sum_{d|(n,k)} f(d)g\left(\frac{k}{d}\right)$，则$S_k(n)$有有限Fourier展式**

$$(7)\quad S_k(n)=\sum_{m \bmod k} a_k(m)e^{\frac{2\pi imn}{k}}.$$

其中

$$(8)\quad a_k(m)=\sum_{d|(m,k)} g(d)f\left(\frac{k}{d}\right)\frac{d}{k}.$$

证明　根据定理8.4，系数$a_k(m)$由

$$a_k(m)=\frac{1}{k}\sum_{n \bmod k} S_k(n)e^{\frac{-2\pi imn}{k}}$$

$$=\frac{1}{k}\sum_{n=1}^{k}\sum_{\substack{d|k\\ d|n}} f(d)g\left(\frac{k}{d}\right)e^{\frac{-2\pi imn}{k}}$$

给定．现在我们写$n=cd$并注意，对每一个固定的d，数c从1变到$\frac{k}{d}$，我们得到

$$a_k(m)=\frac{1}{k}\sum_{d\mid k}f(d)g\left(\frac{k}{d}\right)\sum_{c=1}^{k/d}e^{\frac{-2\pi icdm}{k}}$$

现在我们把右边的和式里$\frac{k}{d}$与d互换，得

$$a_k(m)=\frac{1}{k}\sum_{d\mid k}f\left(\frac{k}{d}\right)g(d)\sum_{c=1}^{d}e^{\frac{-2\pi icm}{d}}$$

但根据定理8.1，当$d\nmid m$时，c上的这个和为0，当$d\mid m$时，这个和的值为d，于是

$$a_k(m)=\frac{1}{k}\sum_{\substack{d\mid k\\ d\mid m}}f\left(\frac{k}{d}\right)g(d)d.$$

这就证明了(8)式成立． □

我们限定f和g为特殊的函数可得到前面的Ramanujan和的公式．

定理8.6 我们有

$$G_k(n)=\sum_{d\mid(n,k)}du\left(\frac{k}{d}\right).$$

证明　在定理8.5里取$f(k)=k$，$g(k)=u(k)$，我们得

$$\sum_{d\mid(n,k)}du\left(\frac{k}{d}\right)=\sum_{m\bmod k}a_k(m)e^{\frac{2\pi imn}{k}}$$

其中

$$a_k(m)=\sum_{d\mid(m,k)}u(d)=\left[\frac{1}{(m,k)}\right]$$

$$=\begin{cases}1 & 如果(m,k)=1\\ 0 & 如果(m,k)>1.\end{cases}$$

于是

$$\sum_{d\mid(n,k)} du\left(\frac{k}{d}\right)=\sum_{\substack{m \bmod k\\(m,k)=1}} e^{\frac{2\pi imn}{k}}=C_k(n). \quad \square$$

8.4 和$S_k(n)$的乘法性质

定理8.7 令

$$S_k(n)=\sum_{d\mid(n,k)} f(d)g\left(\frac{k}{d}\right),$$

其中f和g都是积性函数，则我们有

（9） $S_{mk}(ab)=S_m(a)S_k(b)$ 当$(a,k)=(b,m)=1$时.

特别，我们有

（10） $S_m(a, b)=S_m(a)$ 当$(b,m)=1$时，

与

（11） $S_{mk}(a)=S_m(a)g(k)$ 当$(a,k)=1$时.

证明 由$(a,k)=(b,m)=1$推出（参看习题1.24）

$$(mk, ab)=(a, m)(k, b)$$

以及(a,m)和(b,k)互素. 因此

$$S_{mk}(ab)=\sum_{d\mid(mk,ab)} f(d)g\left(\frac{mk}{d}\right)$$

$$=\sum_{d\mid(m,a)(b,k)} f(d)g\left(\frac{mk}{d}\right).$$

在最后的和式里写$d=d_1d_2$，我们得

$$S_{mk}(ab)=\sum_{d_1\mid(a,m)}\sum_{d_2\mid(b,k)} f(d_1d_2)g\left(\frac{mk}{d_1d_2}\right)$$

$$=\sum_{d_1\mid(a,m)} f(d_1)g\left(\frac{m}{d_1}\right)\sum_{d_2\mid(b,k)} f(d_2)g\left(\frac{k}{d_2}\right)$$

$$=S_m(a)S_k(b).$$

这就证明了(9).

在(9)里取$k=1$，我们得到

$$S_m(ab)=S_m(a)S_1(b)=S_m(a),$$

这是因为$S_1(b)=f(1)g(1)=1$. 在(9)里取$b=1$，并因为$S_k(1)=f(1)g(k)=g(k)$，我们得到

$$S_{mk}(a)=S_m(a)S_k(1)=S_m(a)g(k).$$

这就证明了(11). □

例 对Ramanujan和我们有下列乘法性质：

$C_{mk}(ab)=C_m(a)C_k(b)$ 当$(a, k)=(b,m)=1$时，

$C_m(ab)=C_m(a)$ 当$(b, m)=1$时，

$C_{mk}(a)=C_m(a)\mu(k)$ 当$(a, k)=1$时.

有时可用Dirichlet乘积$f*g$来计算$S_k(n)$，在这方面我们有：

定理8.8 令f是完全积性的，并令 $g(k)=\mu(k)h(k)$，其中h是积性的. 假设对所有的素数p，$f(p)\neq 0$ 并且 $f(p)\neq h(p)$，并令

$$S_k(n)=\sum_{d\mid(n,k)} f(d)g\left(\frac{k}{d}\right),$$

那么，我们有

$$S_k(n)=\frac{F(k)g(N)}{F(N)},$$

其中$F=f*g$，$N=\frac{k}{(n,k)}$.

证明 首先我们注意到

$$F(k)=\sum_{d\mid k} f(d)\mu\left(\frac{k}{d}\right)h\left(\frac{k}{d}\right)$$

$$=\sum_{d\mid k} f\left(\frac{k}{d}\right)\mu(d)h(d)$$

$$=f(k)\sum \mu(d)\frac{h(d)}{f(d)}$$

$$=f(k)\prod_{p\mid k}\left(1-\frac{h(p)}{f(p)}\right).$$

其次，我们写$a=(n,\ k)$，所以$k=aN$，于是我们有

$$S_k(n)=\sum_{d\mid a} f(d)\mu\left(\frac{k}{d}\right)h\left(\frac{k}{d}\right)$$

$$=\sum_{d\mid a} f(d)\mu\left(\frac{aN}{d}\right)h\left(\frac{aN}{d}\right)$$

$$=\sum_{d\mid a} f\left(\frac{a}{b}\right)\mu(Nd)h(Nd).$$

当$(N,\ d)=1$时，$\mu(Nd)=\mu(N)\mu(d)$，而当$(N,\ d)>$时1，$\mu(Nd)=0$. 所以最后的等式给我们

$$S_k(n)=\mu(N)h(N)\sum_{\substack{d\mid a\\(N,d)=1}} f\left(\frac{a}{b}\right)\mu(d)h(d)$$

$$=f(a)\mu(N)h(N)\sum_{\substack{d\mid a\\(N,d)=1}}\mu(d)\frac{h(d)}{f(d)}$$

$$=f(a)\mu(N)h(N)\prod_{\substack{p\mid a\\p\nmid N}}\left(1-\frac{h(p)}{f(p)}\right)$$

$$=f(a)\mu(N)h(N)\frac{\prod\limits_{p\mid a\times 1}\left(1-\frac{h(p)}{f(p)}\right)}{\prod\limits_{p\mid N}\left(1-\frac{h(p)}{f(p)}\right)}$$

$$=f(a)\mu(N)h(N)\frac{F(k)f(N)}{f(k)F(N)}$$

$$=\frac{F(k)\mu(N)h(N)}{F(N)}=\frac{F(k)g(N)}{F(N)}.\qquad \square$$

例 对Ramanujan和我们得到下面的简化式：

$$C_k(n)=\frac{\varphi(k)\mu(N)}{\varphi(N)}=\frac{\varphi(k)\mu\left(\frac{k}{(n,k)}\right)}{\varphi\left(\frac{k}{(n,k)}\right)}.$$

8.5 与Dirichlet特征相伴的Gauss和

定义 对任一Dirichlet特征x modk，和

$$G(n,\ x)=\sum_{m=1}^{k}x(m)e^{\frac{2\pi imn}{k}}$$

称为与x相伴的Gauss和.

如果$x=x_1$是主特征modk，当$(m,\ k)=1$，我们有$x_1(m)=1$，而在其他情况下，$x_1(m)=0$，这样，Gauss和简化为Ramanujan和：

$$G(n,\ x_1)=\sum_{\substack{m=1\\(m,k)=1}}^{k}e^{\frac{2\pi imn}{k}}=C_k(n).$$

即Gauss和$G(n,\ x)$能看作是Ramanujan和的推广. 现在我们转而详细地研究它的性质.

首先一个结果是因式分解的性质. 它在子序列的展开式中起着重要的作用.

定理8.9 如果x是任一Dirichlet特征modk，则有

$$G(n,\ x)=\overline{x(n)}G(1,\ x)\quad 当(n,\ k)=1时.$$

证明 当$(n,\ k)=1$时，数nr随着r一起通过模k的一个完全剩余系，而且$|x(n)|^2=x(n)\overline{x}(n)=1$，所以，

$$x(r)=\overline{x}(n)x(n)x(r)=\overline{x}(n)x(nr).$$

因此，定义的G(n，x)的和能写为如下形式：

$$G(n, x)=\sum_{r \bmod k} x(r)e^{\frac{2\pi i n r}{k}}$$

$$=\overline{x}(n)\sum_{r \bmod k} x(nr)e^{\frac{2\pi i n r}{k}}$$

$$=\overline{x}(n)\sum_{m \bmod k} x(m)e^{\frac{2\pi i m}{k}}$$

$$=\overline{x}(n)G(1, x).$$

定理得证. □

定义 Gauss和G(n，x)说是可分的，如果

(12) $G(n, x)=\overline{x}(n)G(1, x)$.

定理8.9 告诉我们，当n与模k互素时，G(n，x)是可分的．对于与k不互素的那些n，我们有下面的定理．

定理8.10 如果x是一个特征modk，则对每一个n，G(n，x)是可分的当且仅当

$G(n, x)=0$ 在$(n, k)>1$时．

证明 当(n，k)=1时，可分性始终是成立的．但若(n，k)>1，我们有$\overline{x}(n)=0$，所以等式(12)成立当且仅当$G(n, x)=0$. □

下面的定理给出可分性的一个重要推论．

定理8.11 如果G(n，x)对所有的n都是可分的，则有

(13) $|G(1, \chi)|^2=k$.

证明 我们有

$$|G(1, \chi)|^2=G(1, \chi)\overline{G(1, \chi)}$$

$$=G(1, \chi)\sum_{m=1}^{k}\overline{\chi}(m)e^{\frac{-2\pi i m}{k}}$$

$$=\sum_{m=1}^{k} G(m, \chi)e^{\frac{-2\pi i m}{k}}$$

$$=\sum_{m=1}^{k}\sum_{r=1}^{k}\chi(r)e^{\frac{2\pi i m r}{k}}e^{\frac{-2\pi i m}{k}}$$

$$=\sum_{r=1}^{k}\chi(r)\sum_{m=1}^{k}e^{\frac{2\pi i m(r-1)}{k}}$$

$$=k\chi(1)=k.$$

因为最后一个m上的和式是一个几何和，除r＝1之外，它的值为零.

8.6 具有非零Gauss和的Dirichlet特征

对模k的每一个特征x，我们看到，当(n, k)＝1时，G(n, x)是可分的．对于(n, k)>1，G(n, k)可分等价于G(n, k)为零．现在我们描述，在(n, k)>1时，满足G(n, x)＝0的特征x的进一步的性质。实际上，研究G(n, x)≠0的x更简单．下面的定理给出对于(n, k)>1，G(n, x)非零的必要条件．

定理8.12　令x是Dirichlet特征 modk，并设对于满足(n, k)>1的某个n，有G(n, x)≠0．那么存在k的一个因数d，d<k，使得

(14)　x(a)＝1，这里(a, k)＝1且a≡1(modd)

证明　对于给定的n，令q＝(n, k)，$d=\frac{k}{q}$，于是d|k，又因q>1，我们有d<k．选择任一满足(a, k)＝1与a≡1(mod d)的a，我们将证明x(a)＝1．

因为(a, k)＝1，在定义G(n, x)的和里，我们可以把指标m换为am，我们得到

$$G(n, x)=\sum_{m \bmod k} x(m)e^{\frac{2\pi inm}{k}}$$
$$=\sum_{m \bmod k} x(am)e^{\frac{2\pi inam}{k}}$$
$$=x(a)\sum_{m \bmod k} x(m)e^{\frac{2\pi inam}{k}}.$$

因为$a\equiv 1 \pmod d$并且$d=\frac{k}{q}$，我们能够写$a=1+\left(\frac{bk}{q}\right)$，b是整数，我们有

$$\frac{anm}{k}=\frac{nm}{k}+\frac{bknm}{qk}=\frac{nm}{k}+\frac{bnm}{q}$$
$$\equiv\frac{nm}{k} \pmod 1$$

这因为$q|n$。于是$e^{\frac{2\pi ianm}{k}}=e^{\frac{2\pi inm}{k}}$并且$G(n, x)$的和变为

$$G(n, x)=x(a)\sum_{m \bmod k} x(m)e^{\frac{2\pi inm}{k}}$$
$$=x(a)G(n, x).$$

因为$G(n, x)\neq 0$，得出$x(a)=1$。 □

上面的定理引导我们去考虑模k的某些特征，对这些特征，有k的一个因数$d<k$满足(14)。这就是下面的讨论。

8.7 诱导模与本原特征

诱导模的定义　令χ是一个Dirichlet特征modk，并令d是k的任一正因数。数d叫做是x的一个诱导模，如果当$(a, k)=1$且$a\equiv 1 \pmod d$时，我们有

(15) $x(a)=1$.

换言之，如果模k的特征x与模d的一个特征在模d的剩

余类$\hat{1}$所表示的数上作用相同，而这些数是与k互素的，则d是一个诱导模.

注意，k自身对于χ总是一个诱导模.

定理8.13 令χ是模k的一个Dirichlet特征. 则1对于χ是一个诱导模当且仅当$\chi=\chi_1$.

证明 如果$\chi=\chi_1$，则对所有与k互素的a，有$\chi(a)=1$. 但因每一个a均满足$a\equiv 1 \pmod 1$，故数1是一个诱导模.

反之，如果1是一个诱导模，则当$(a, k)=1$时，$\chi(a)=1$，所以$\chi=\chi_1$，因为在与k不互素的数上，χ为零.

对模k的任一Dirichlet特征，模k自身是一个诱导模. 如果它没有别的诱导模，我们就称这样的特征是本原的，这样，我们有

本原特征的定义 模k的一个Dirichlet特征叫做是本原的mod k，如果它没有诱导模$d<k$. 换言之，χ是本原的mod k，当且仅当，对k的每一个因数d，$0<d<k$，存在一个整数$a\equiv 1 \pmod d$ $(a, k)=1$，使$\chi(a)\neq 1$.

如果$k>1$，则主特征χ_1是非本原的，因为它有1是诱导模. 下面我们证明，如果模是素数，则每一个非主特征都是本原的.

定理8.14 素数模p的每一个非主特征都是本原特征mod p.

证明 p仅有因数1和p，所以只有这两个数可能为诱导模. 但如果$\chi\neq\chi_1$，则约数1不是诱导模，所以χ没有$<p$的诱导模，于是χ是本原的.

现在我们用本原特征的说法来重新叙述从定理8.10至定

理8.12的结果.

定理8.15 令χ是一个本原的Dirichlet特征 mod$k$，那么我们有

(a) $G(n, \chi)=0$ 对每一个具有$(n, k)>1$的n.

(b) $G(n, \chi)$是可分的 对每一个n.

(c) $|G(1, \chi)|^2=k$.

证明 如果对某个满足$(n, k)>1$的n，$G(n, \chi)\neq 0$，那么由定理8.12得出χ有一个诱导模$d<k$，所以χ不是本原的，这个矛盾证明了(a)成立. 由(a)与定理8.10立即得出(b). 由(b)与定理8.11立即得出(c).

注: 定理8.15(b)指出，当χ是本原的时，Gauss和$G(n, \chi)$是可分的.在后面我们将证明它的逆，即如果对每一个n，$G(n, \chi)$是可分的，则χ是本原的.（参看定理8.19）.

8.8 诱导模的进一步的性质

下面的定理论及χ在一些数上的作用，这些数对于以诱导模为模是同余的.

定理8.16 令χ是一个Dirichlet特征mod$k$，并设$d|k$，$d>0$，那么d对χ是诱导模当且仅当(16) $\chi(a)=\chi(b)$. 其中$(a, k)=(b, k)=1$，且$a\equiv b \pmod d$.

证明 如果(16)成立，则d是一个诱导模，因为我们可以选取$b=1$并利用(15)式. 现在我们证明其逆.

选取a与b使$(a,k)=(b,k)=1$并且$a\equiv b \pmod d$. 我们将证明$\chi(a)=\chi(b)$.令a'与a互逆mod$k$，即$aa'\equiv 1 \pmod k$. 因为$(a, k)=1$，所以这个逆a'存在. 因为$d|k$，所以$aa'\equiv$

$1 \pmod d$. 因为d是一个诱导模，于是$\chi(aa')=1$. 但$aa' \equiv ba' \equiv 1 \pmod d$，这因为$a \equiv b \pmod d$. 于是$\chi(aa') \equiv \chi(ba')$ 所以

$$\chi(a)\chi(a')=\chi(b)\chi(a').$$

但因$\chi(a)\chi(a')=1$，所以$\chi(a')\neq 0$. 消去$\chi(a')$后，我们得到$\chi(a)=\chi(b)$. 证明完成. □

(16)式告诉我们，在与k互素的那些数上，χ是周期函数mod d. 这样，χ的作用很象模d的一个特征. 为了进一步研究这个关系，讨论几个例子是有意义的.

例 1 下面的表列出了模 9 的一个特征.

n	1	2	3	4	5	6	7	8	9
$\chi(n)$	1	−1	0	1	−1	0	1	−1	0

我们注意，这个表以模3为周期，所以3是χ的一个诱导模. 实际上，χ的作用与下面模3的特征ψ相同:

n	1	2	3
$\psi(n)$	1	−1	0

因为对所有的n，有$\chi(n)=\psi(n)$，所以我们称χ是ψ的一个延伸. 显然，当χ是模d的一个特征ψ的延伸时，则d是χ的一个诱导模.

例 2 现在我们考察模6的一个特征χ:

n	1	2	3	4	5	6
$\chi(n)$	1	0	0	0	−1	0

在这种情况下，因为对所有的$n \equiv 1 \pmod 3$，$(n, 6)=1$，有$\chi(n)=1$，所以数3是一个诱导模.（仅有一个这样的n，即n=1）. 可是χ不是模3的任何一个特征ψ的延伸，因

为模3唯一的特征是主特征ψ_1，它由下表给定：

n	1	2	3
$\psi_1(n)$	1	1	0

而特征ψ在例1里已经给出．因为$\chi(2)=0$，所以χ不能是ψ_1或ψ的延伸．

这两个例子说明了下面的定理．

定理8.17 **令χ是模k的一个Dirichlet特征，并设$d|k$，$d>0$，那么下面两条是等价的：**

(a) d是χ的一个诱导模．

(b) 存在模d的一个特征ψ，使得

(17) $\chi(n)=\psi(n)\chi_1(n)$

对所有的n成立，其中χ_1是模k的主特征．

证明　假设(b)成立，选择n，使$(n, k)=1$，$n\equiv 1 \pmod d$，则$\chi_1(n)=\psi(n)=1$，所以$\chi(n)=1$，于是d是一个诱导模．这样，由(b)推出了(a)．

现在假设(a)成立，我们可以找出一个特征$\psi \bmod d$，使(17)式成立．我们如下定义$\psi(n)$：如果$(n, d)>1$，则令$\psi(n)=0$，这时也有$(n, k)>1$，因为两端为零，所以这时(17)成立．

现在我们假设$(n, d)=1$，则存在一个整数m，使$m\equiv n \pmod d$，$(m, k)=1$．这能由Dirichlet定理立即得到证实．因为算术级数$xd+n$中有无穷多个素数，我们可选择一个除不尽k的这样的素数并记为m．于是，结论是不难理解的．这样的m的存在性不用Dirichlet定理也容易确定．（作为一个代替的证明请参看习题8.4）．所选出的m，对于模d

是唯一的．我们规定

$$\psi(n)=\chi(m).$$

因为在与k互素并对模d同余的那些数上，χ取得相同的值，所以数$\psi(n)$是完全确定的．

实际上，读者容易验证，χ是模d的一个特征．下面我们证明，对所有的n，(17)式都成立．

如果$(n, k)=1$，则$(n, d)=1$，所以对$m\equiv n \pmod d$，有$\psi(n)=\chi(m)$，于是根据定理8.16，因为$\chi_1(n)=1$，有

$$\chi(n)=\chi(m)=\psi(n)=\psi(n)\chi_1(n).$$

如果$(n, k)>1$，则$\chi(n)=\chi_1(n)=0$，并且(17)两端都是零．所以(17)对所有的n成立．　□

8.9 特征的前导子

定义　令χ是模k的Dirichlet特征．χ的最小诱导模称为是χ的前导子．

定理8.18　模k的每一个Dirichlet特征能表为乘积式

$$(18)\qquad \chi(n)=\psi(n)\chi_1(n)\quad \text{对所有的}n.$$

其中χ_1是模k的主特征而ψ是以χ的前导子为模的本原特征．

证明　令d是χ的前导子，由定理8.17我们知道，χ能表为形如(18)的乘积，其中ψ是模d的特征．现在我们证明ψ是模d的本原特征．

我们假设ψ不是模d的本原特征并得出一个矛盾．如果ψ对模d不是本原的，则存在d的一个约数$q<d$，它是ψ的一个诱导模．我们将证明这个q也整除k并且也是χ的一个诱导模，这与d是χ的最小诱导模矛盾．

选择$n\equiv 1 \pmod q$，$(n, k)=1$，于是

$$\chi(n)=\psi(n)\chi_1(n)=\psi(n)=1,$$

这因为q是ψ的一个诱导模．于是q也是χ的一个诱导模，这是一个矛盾．

8.10 本原特征与可分的Gauss和

作为前述定理的一个应用，下面我们给出本原特征的一个替换描述．

定理8.19 令χ是模k的一个特征，则χ是模k的本原特征当且仅当Gauss和

$$G(n, \chi)=\sum_{m \bmod k}\chi(m)e^{\frac{2\pi imn}{k}}$$

对每个n都是可分的．

证明 如果χ是本原的，则根据定理8.15(b)，$G(n, \chi)$是可分的．现在我们证明其逆．

根据定理8.9与8.10，只要我们能证明，当χ对模k为非本原时，有某个满足$(r, k)>1$的r，使$G(r,)\chi\neq 0$，那么本定理的证明就完成了．于是假设χ对模k是非本原的，这意指$k>1$，于是x有一个前导子$d<k$．令$r=\frac{k}{d}$，则$(r, k)>1$，下面我们证明，对这个r，$G(r, \chi)\neq 0$．

根据定理8.18，存在模d的一个本原特征ψ，使得对所有的n，有$\chi(n)=\psi(n)\chi_1(n)$，于是我们可写

$$G(r, \chi)=\sum_{m \bmod k}\psi(m)\chi_1(m)e^{\frac{2\pi irm}{k}}$$

$$=\sum_{\substack{m \bmod k\\(m, k)=1}}\psi(m)e^{\frac{2\pi irm}{k}}$$

$$= \sum_{\substack{m \bmod k \\ (m,k)=1}} \psi(m) e^{\frac{2\pi i m}{d}}$$

$$= \frac{\varphi(k)}{\varphi(d)} \sum_{\substack{m \bmod d \\ (m,d)=1}} \psi(m) e^{\frac{2\pi i m}{d}},$$

其中，最后一步我们利用了定理5.33(a)．因此，我们有

$$G(r, x) = \frac{\varphi(k)}{\varphi(d)} G(1, \psi).$$

但根据定理8.15，$|G(1, \psi)|^2 = d$（因为ψ对模d是本原的）．因而$G(r, x) \neq 0$．证明完成。 □

8.11 Dirichlet特征的有限Fourier级数

因为模k的每一个Dirichlet特征都是周期的 modk，所以它有有限Fourier展开式

$$(19) \quad \chi(m) = \sum_{n=1}^{k} a_k(n) e^{\frac{2\pi i m n}{k}},$$

定理8.4还告诉我们，它的系数由公式

$$a_k(n) = \frac{1}{k} \sum_{m=1}^{k} \chi(m) e^{\frac{-2\pi i m n}{k}}$$

给定．其右端的和是Gauss和$G(-n, x)$，所以我们有

$$(20) \quad a_k(n) = \frac{1}{k} G(-n, x).$$

当χ是本原的时候，Fourier展开式(19)能表示如下：

定理8.20　模k的本原Dirichlet特征χ的有限Fourier展开式有形式

$$(21) \quad \chi(m) = \frac{\tau_k(\chi)}{\sqrt{k}} \sum_{n=1}^{k} \overline{\chi}(n) e^{\frac{-2\pi i m n}{k}},$$

其中

(22) $\tau_k(\chi)=\frac{G(1,\chi)}{\sqrt{k}}=\frac{1}{\sqrt{k}}\sum_{m=1}^{k}\chi(m)e^{\frac{2\pi i m}{k}}$.

数$\tau_k(\chi)$的绝对值为1.

证明　因为χ是本原的，所以我们有$G(-n,\chi)=\overline{\chi}(n)G(1,\chi)$，又由(20)得出$a_k(n)=\frac{\overline{\chi}(-n)G(1,\chi)}{k}$.

因此(19)能写为

$$\chi(m)=\frac{G(1,\chi)}{k}\sum_{n=1}^{k}\overline{\chi}(-n)e^{\frac{2\pi i m n}{k}}$$

$$=\frac{G(1,\chi)}{k}\sum_{n=1}^{k}\overline{\chi}(n)e^{\frac{-2\pi i m n}{k}},$$

这与(21)式相同. 由定理8.11说明$\tau_k(\chi)$的绝对值为1. □

8.12　本原特征部分和的Pólya不等式

在第七章给出的Dirichlet定理的证明中利用了关系式

$$\left|\sum_{m\leqslant x}\chi(m)\right|\leqslant\varphi(k),$$

它对模k的任一Dirichlet特征与每一个实数$x\geqslant1$成立. 当$\chi=\chi_1$时，因为$\sum_{m=1}^{k}\chi_1(m)=\varphi(k)$，所以这个不等式不能改进了. 但是Pólya证明了，当是一个本原特征时，这个不等式有一个大的改进.

定理8.21　Pólya不等式. 如果χ是模k的任一本原特征，那么对所有$x\geqslant1$，我们有

(23) $\left|\sum_{m\leqslant x}\chi(m)\right|<\sqrt{k}\log k$.

证明　我们用有限Fourier展开式来表示$\chi(m)$，由定理

8.20给出

$$\chi(m)=\frac{\tau_k(\chi)}{\sqrt{k}}\sum_{n=1}^{k}\overline{\chi}(n)e^{\frac{-2\pi imn}{k}},$$

并对所有$m\leqslant x$求和，得出

$$\sum_{m\leqslant x}\chi(m)=\frac{\tau_k(\chi)}{\sqrt{k}}\sum_{n=1}^{k-1}\overline{\chi}(n)\sum_{m\leqslant x}e^{\frac{-2\pi imn}{k}},$$

这因为$\chi(k)=0$. 再取绝对值并用$\sqrt{k}$去乘，我们得到

$$(24)\quad \sqrt{k}\left|\sum_{m\leqslant x}\chi(m)\right|\leqslant\sum_{n=1}^{k-1}\left|\sum_{m\leqslant x}e^{\frac{-2\pi imn}{k}}\right|$$

$$=\sum_{n=1}^{k-1}|f(n)|,$$

其中，

$$f(n)=\sum_{m\leqslant x}e^{\frac{-2\pi imn}{k}}.$$

于是

$$f(k-n)=\sum_{m\leqslant x}e^{\frac{-2\pi im(k-n)}{k}}=\sum_{m\leqslant x}e^{\frac{2\pi imn}{k}}=\overline{f(n)},$$

所以，$|f(k-n)|=|f(n)|$. 于是(24)可写为

$$(25)\quad \sqrt{k}\ \left|\sum_{m\leqslant x}\chi(m)\right|\leqslant 2\sum_{n\leqslant\frac{k}{2}}|f(n)|.$$

于是，$f(n)$是一个形如

$$f(n)=\sum_{m=1}^{r}y^m$$

的几何和．其中$r=[x]$，$y=e^{\frac{-2\pi in}{k}}$. 因为$1\leqslant n\leqslant k-1$，所以$y\neq 1$. 写$z=e^{\frac{-\pi in}{k}}$，我们有$y=z^2$，并因$n\leqslant\frac{k}{2}$，$z^2\neq 1$. 于是我们有

$$f(n)=y\frac{y^r-1}{y-1}=z^2\frac{z^{2r}-1}{z^2-1}=z^{r+1}\frac{z^r-z^{-r}}{z-z^{-1}},$$

所以有

$$(26)\quad |f(n)| = \left|\frac{z^{r}-z^{-r}}{z-z^{-1}}\right| = \left|\frac{e^{\frac{-\pi i r n}{k}}-e^{\frac{\pi i r n}{k}}}{e^{\frac{-\pi i n}{k}}-e^{\frac{\pi i n}{k}}}\right|$$

$$=\frac{\left|\sin\frac{\pi r n}{k}\right|}{\left|\sin\frac{\pi n}{\pi}\right|}\leqslant\frac{1}{\sin\frac{\pi n}{k}}.$$

现在我们利用不等式 $\sin t\geqslant\frac{2t}{\pi}$，它对于$0\leqslant t\leqslant\frac{\pi}{2}$与$t=\frac{\pi n}{k}$是正确的，得到

$$|f(n)|\leqslant\frac{1}{\frac{2}{\pi}\ \frac{\pi n}{k}}=\frac{k}{2n}.$$

于是(25)变为

$$\sqrt{k}\ \left|\sum_{m\leqslant x}\chi(m)\right|\leqslant k\sum_{n\leqslant\frac{k}{2}}\frac{1}{n}<k\log k,$$

这证明了(23)． □

注：在后面的章节里我们将证明，Pólya不等式能推广为对任意非主特征。对于非本原特征，它有形式

$$\sum_{m\leqslant x}\chi(m)=0(\sqrt{k}\log k).$$

（参看定理13·15）

第八章 习 题

1． 令$x=e^{\frac{2\pi i}{n}}$，证明

$$\sum_{k=1}^{n-1}kx^{k}=\frac{n}{x-1}.$$

2． 当x不是整数时，令$((x))=x-[x]-\frac{1}{2}$. 在其他情况

下，令$((x))=0$．注意，$((x))$是x的周期为1的周期函数．如果k和n都是整数，并且$n>0$，证明

$$\left(\left(\frac{k}{n}\right)\right)=-\frac{1}{2n}\sum_{m=1}^{n-1}\cot\frac{\pi m}{n}\sin\frac{2\pi km}{n}.$$

3． 令$C_k(m)$表示Ramanujan和，并令$M(x)=\sum_{n\leqslant x}\mu(n)$为Möbius函数的部分和．

(a) 证明

$$\sum_{k=1}^{n}C_k(m)=\sum_{d\mid m}dM\left(\frac{n}{d}\right),$$

特别，当$n=m$时，我们有

$$\sum_{k=1}^{m}C_k(m)=\sum_{d\mid m}dM\left(\frac{m}{d}\right).$$

(b)利用(a)推出

$$M(m)=m\sum_{d\mid m}\frac{\mu\left(\frac{m}{d}\right)}{d}\sum_{k=1}^{d}C_k(d).$$

(c)证明

$$\sum_{m=1}^{n}C_k(m)=\sum_{d\mid k}d\mu\left(\frac{k}{d}\right)\left[\frac{n}{d}\right].$$

4． 令n，a，d是给定的整数并且$(a, d)=1$．又令$m=a+qd$，其中q是除尽n但不能除尽a的所有素数的乘积（可能是空的）．证明

$$m\equiv a\ (\mathrm{mod}\ d)\ \text{并且}\ (m, n)=1.$$

5． 如果m是奇数，$k=2m$，证明，存在模k的一个非实本原特征．

6． 令χ是模k的一个特征．如果k_1和k_2是χ的诱导模，证明，k_1，k_2的最大公约数(k_1, k_2)也是χ的诱导模．

7． 证明χ的前导子除尽χ的每一个诱导模．

在8至12题里，假设$k=k_1k_2\cdots k_r$，其中正整数k_i是两两互素的：$(k_i, k_j)=1$，$i\neq j$.

8. (a)给定任一整数a，证明存在一个整数a_i，使得$a_i\equiv a \pmod{k_i}$并且$a_i\equiv 1 \pmod{k_j}$对所有$j\neq i$.

(b) 令χ是模k的一个特征．由等式

$$\chi_i(a)=\chi(a_i)$$

定义χ_i，其中a_i是(a)部分里的整数．证明χ_i是模k_i的特征．

9. 证明模k的每一个特征能够唯一地表为因子乘积的形式$\chi=\chi_1\chi_2\cdots\chi_r$，其中$\chi_i$是$k_i$的特征．

10. 令$f(\chi)$表示χ的前导子．如果χ有第9题的因子分解式，证明，$f(\chi)=f(\chi_1)\cdots f(\chi_r)$.

11. 如果χ有第9题的因子分解式，证明，对每一个整数a，我们有

$$G(a, \chi)=\prod_{i=1}^{r}\chi_i\left(\frac{k}{k_i}\right)G(a_i, \chi_i),$$

其中a_i是第8题里的整数．

12. 如果χ_i有第9题里的因子分解式，证明χ是本原的 mod k，当且仅当每一个χ_i是本原的 mod k_i．［提示，定理8.19］．

13. 令χ是模k的本原特征，证明，当N<M时，我们有

$$\left|\sum_{m=N+1}^{M}\frac{\chi(m)}{m}\right|<\frac{2}{N+1}\sqrt{k}\log k .$$

14. 这个题描述了Pólya不等式的一个小的改进．可参阅定理8.21的证明．由不等式(26)，可写

$$\sum_{n<\frac{k}{2}}|f(n)|\leqslant\sum_{n\leqslant\frac{k}{2}}\frac{1}{\sin\frac{\pi n}{k}}<\frac{1}{\sin\frac{\pi}{k}}+\int_1^{\frac{k}{2}}\frac{dt}{\sin\frac{\pi t}{k}}.$$

证明这个积分小于$-\left(\frac{k}{\pi}\right)\log\left(\sin\left(\frac{\pi}{2k}\right)\right)$并推出

$$\left|\sum_{n\leqslant x}x(n)\right|<\sqrt{k}+\frac{2}{\pi}\sqrt{k}\log k.$$

由于商$\frac{2}{\pi}$在主项里，这改进了Pòlya不等式.

15．Kloosterman和$K(m,n;k)$定义如下：

$$K(m,n;k)=\sum_{\substack{h \bmod k\\(t,k)=1}}e^{\frac{2\pi i(n'h+nh')}{k}},$$

其中h'是h的倒数mod k．当$k|n$时，这简化为Ramanujan和$C_k(m)$．推出下列Kloosterman和的性质：

(a) $k(m,n;k)=k(n,m;k)$.

(b) $k(m,n;k)=k(1,mn;k)$　其中$(m,k)=1$.

(c) 给定整数n，k_1，k_2，$(k_1,k_2)=1$．证明，存在整数n_1和n_2，使得

$$n\equiv n_1k_2^2+n_2k_1^2\quad(\bmod k_1k_2),$$

并且对这些整数，我们有

$$k(m,n;k_1k_2)=k(m,n_1;k_1)K(m,n_2;k_2).$$

这归结为研究特殊情形的Kloosterman和$K(m,n;p^\alpha)$，其中p是素数.

16．如果n和k是整数，$n>0$，则和

$$G(k;\ n)=\sum_{r=1}^{n} e^{\frac{2\pi i k r^2}{n}}$$

称为二次Gauss和．推出二次Gauss和的下列性质：

(a) $G(k;\ mn)=G(km;\ n)G(kn;\ m)$当$(m,\ n)=1$时．

这归结为研究特殊情况的Ganss和$G(k;\ p^{\alpha})$，其中P是素数．

(b) 令p是一个奇素数，$p\nmid k$，$\alpha\geqslant 2$，证明$G(k;\ p^{\alpha})=pG(k;\ p^{\alpha-2})$，并推出

$$G(k;\ p^{\alpha})=\begin{cases} p^{\frac{\alpha}{2}} & \alpha\text{为偶数}, \\ p^{\frac{(\alpha-1)}{2}}G(k;\ p) & \alpha\text{为奇数}. \end{cases}$$

Gauss和$G(k;\ p)$的进一步的性质出现在下一章里．在那里，证明了$G(k;\ p)$等于与模p的某个Dirichlet 特征χ相伴的Gauss和$G(k,\ x)$．（参看习题9.9．）

第九章　二次剩余与二次互反律

9.1　二次剩余

我们在第五章里曾经指出，解一个多项式同余式

$$f(x)\equiv 0 \pmod{m}$$

的问题能简化为解具有素数模的一些同余式加上一组一次同余式．本章讨论形如

(1) $x^2\equiv n \pmod{p}$

的二次同余式，其中 p 是一个奇素数并且 $n\not\equiv 0 \pmod{p}$．因为模是素数，我们知道(1)最多只有两个解．而且，如果 x 是解，则 $-x$ 也是解，于是解的个数是 0 或 2．

定义　如果同余式(1)有解，我们就说 n 是模 p 的二次剩余，并记为 nRp．如果(1)没有解，我们就说 n 是模 P 的二次非剩余，并记为 $n\bar{R}p$．

两个基本问题在二次剩余理论中占支配地位．

1．给定一个素数 p，确定哪些 n 是模 p 的二次剩余，哪些 n 是模 P 的二次非剩余．

2．给定 n，确定素数 p，对这些 p，n 是模 p 的二次剩余，而对另外那些素数 p，n 是模 p 的二次非剩余．

我们从解决问题1的一些方法着手.

例如，为找出模11的二次剩余，我们把数1，2，…，10分别平方并简化为11以内的数，我们得

$$1^2\equiv1,\ 2^2\equiv4,\ 3^2\equiv9,\ 4^2\equiv5,\ 5^2\equiv3\ (\mathrm{mod}11).$$

只要这前面一半的平方数就够了，因为

$$6^2\equiv(-5)^2\equiv3,\ 7^2\equiv(-4)^2\equiv5,$$

$$10^2\equiv(-1)^2\equiv1(\mathrm{mod}11).$$

所以，模11的二次剩余是1，3，4，5，9而二次非剩余是2，6，7，8，10.

这个例子说明了下面的定理.

定理9.1　令P是一个素数，则模P的任一简化剩余系恰好包含了模P的$\frac{(p-1)}{2}$个二次剩余与$\frac{(p-1)}{2}$个二次非剩余. 包含数

(2)　$1^2,\ 2^2,\ 3^2,\ \cdots\left(\frac{p-1}{2}\right)^2$

的剩余类就是模P的全部二次剩余.

证明　首先，我们注意(2)中各数对模p互不同余. 实际上，如果$x^2\equiv y^2$ (modp)，$1\leqslant x\leqslant\frac{(p-1)}{2}$，$1\leqslant y\leqslant\frac{(P-1)}{2}$，则

$$(x-y)(x+y)\equiv0\quad(\mathrm{mod}p).$$

但$1<x+y<p$，所以$x-y\equiv0$ (modp)，于是$x=y$. 因为

$$(p-K)^2\equiv K^2\quad(\mathrm{mod}p)$$

所以，任何一个二次剩余恰与(2)中之一数同余modp.证明完成. □

下面列的二次剩余 R与二次非剩余$\overline{R}$的短表是借助于定

理9.1得到的.

	p=3	p=5	p=7
R:	1	1, 4	1, 2, 4
$\overline{R}$:	2	2, 3	3, 5, 6

	p=11	p=13
R:	1, 3, 4, 5, 9	1, 3, 4, 9, 10, 12
$\overline{R}$:	2, 6, 7, 8, 10	2, 5, 6, 7, 8, 11

9.2 Legendre符号及其性质

定义 令p是一个奇素数，如果$n\not\equiv 0 \pmod p$，我们定义Legendre符号$\left(\frac{n}{p}\right)$如下：

$$\left(\frac{n}{p}\right)=\begin{cases}+1 & \text{当}nRp\text{时},\\ -1 & \text{当}n\overline{R}p\text{时}.\end{cases}$$

如果$n\equiv 0 \pmod p$，我们规定$\left(\frac{n}{p}\right)=0$.

例：$\left(\frac{1}{p}\right)=1$，$\left(\frac{m^2}{p}\right)=1$，$\left(\frac{7}{11}\right)=-1$，$\left(\frac{22}{11}\right)=0$.

注意：有些作者写为$\left(\frac{n}{p}\right)$以代替(n/p).

显然，当$m\equiv n \pmod p$时，$\left(\frac{m}{p}\right)=\left(\frac{n}{p}\right)$.所以$\left(\frac{n}{P}\right)$是n的周期函数，其周期为P.

Fermat小定理告诉我们，当$p\nmid n$时，$n^{p-1}\equiv 1 \pmod p$.又因

$$n^{p-1}-1=\left(n^{\frac{(p-1)}{2}}-1\right)\left(n^{\frac{(p-1)+1}{2}}+1\right),$$

所以得 $n^{\frac{(p-1)}{2}} \equiv \pm 1 \pmod p$．下面的定理告诉我们，如果$nRp$，则它是1，如果$n\overline{R}p$，则它是$-1$．

定理9.2 Euler准则．令p是一个奇素数，则对所有的n，我们有

$$\left(\frac{n}{p}\right) \equiv n^{\frac{(p-1)}{2}} \pmod p.$$

证明　如果$n\equiv 0 \pmod p$，因为两边都同余于0，故结论成立．现在设$\left(\frac{n}{p}\right)=1$，则存在一个x，使$x^2\equiv n \pmod p$，于是

$$n^{\frac{(p-1)}{2}} \equiv (x^2)^{\frac{(p-1)}{2}} = x^{p-1} = \left(\frac{n}{p}\right) \pmod p,$$

这证明定理在$\left(\frac{n}{p}\right)=1$时成立．

现在假设$\left(\frac{n}{p}\right)=-1$，考虑多项式

$$f(x)= x^{\frac{(p-1)}{2}}-1,$$

因为f(x)的次数为$\frac{(p-1)}{2}$，故同余式

$$f(x)\equiv 0 \pmod p$$

最多只有$\frac{(p-1)}{2}$个解．但模p的$\frac{(p-1)}{2}$个二次剩余都是解，所以二次非剩余不是解，于是

$$n^{\frac{(p-1)}{2}} \not\equiv 1 \pmod p \text{当}\left(\frac{n}{p}\right)=-1\text{时}.$$ 但 $n^{\frac{(p-1)}{2}} \equiv \pm 1 \pmod p$，所以$n^{\frac{(p-1)}{2}} \equiv -1 \equiv \left(\frac{n}{p}\right) \pmod p$．□

证明完成．

定理9.3 Legendre符号$\left(\frac{n}{p}\right)$是n的完全积性函数.

证明 如果$P|m$或$p|n$，则$p|mn$，所以$\left(\frac{mn}{p}\right)=0$且$\left(\frac{m}{p}\right)=0$或者$\left(\frac{n}{p}\right)=0$. 因此，在$P|m$或$P|n$时，$\left(\frac{mn}{p}\right)=\left(\frac{m}{p}\right)\left(\frac{n}{p}\right)$.

如果$p\nmid m$并且$p\nmid n$，则$p\nmid mn$，并有

$$\left(\frac{mn}{p}\right)\equiv(mn)^{\frac{(P-1)}{2}}=m^{\frac{(P-1)}{2}}n^{\frac{(P-1)}{2}}\equiv\left(\frac{m}{p}\right)\left(\frac{n}{p}\right)$$

$(\bmod p)$. 但$\left(\frac{mn}{p}\right)$, $\left(\frac{m}{p}\right)$, $\left(\frac{n}{p}\right)$的每一个只能是$+1$或-1，所以差

$$\left(\frac{mn}{p}\right)-\left(\frac{m}{p}\right)\left(\frac{n}{p}\right)$$

只能是0，2或-2. 因为这个差被p整除，所以它必定为0，等号成立. □

注: 因为$\left(\frac{n}{p}\right)$是n的一个完全积性函数，它又是周期为p的周期函数，并且当$p|n$时，它为0，由此得出$\left(\frac{n}{p}\right)=x(n)$，其中x是模P的一个Dirichlet特征. Legendre符号称为模p的二次特征.

9.3 $\left(-\frac{1}{P}\right)$与$\left(\frac{2}{P}\right)$的值

定理9.4 对任一奇素数P，我们有

$$\left(\frac{-1}{p}\right)=(-1)^{\frac{(P-1)}{2}}=\begin{cases}1 & \text{当}p\equiv1\ (\bmod 4)\text{时，}\\ -1 & \text{当}p\equiv3\ (\bmod 4)\text{时。}\end{cases}$$

证明　根据Euler准则，我们有$\left(\frac{-1}{p}\right)\equiv(-1)^{\frac{(p-1)}{2}}$ $(\bmod p)$，因为这个同余式两边是1或-1，所以两部分相等.

定理9.5　对任一奇素数p，我们有

$$\left(\frac{2}{p}\right)=(-1)^{\frac{(p^2-1)}{8}}=\begin{cases}1 & \text{当}p\equiv\pm1(\bmod 8)\text{时,}\\ -1 & \text{当}p\equiv\pm3(\bmod 8)\text{时.}\end{cases}$$

证明　考虑下面$\frac{(P-1)}{2}$个同余式：

$$\begin{aligned}
p-1&\equiv1(-1)^1 &(\bmod p)\\
2&\equiv2(-1)^2 &(\bmod p)\\
p-3&\equiv3(-1)^3 &(\bmod p)\\
4&\equiv4(-1)^4 &(\bmod p)\\
&\vdots\\
r&\equiv\frac{p-1}{2}(-1)^{\frac{(p-1)}{2}} &(\bmod p),
\end{aligned}$$

其中r是$P-\frac{(p-1)}{2}$或$\frac{(p-1)}{2}$. 把这些式子乘在一起，注意左边每个数都是偶数，我们得到

$$2\cdot4\cdot6\cdots(p-1)\equiv\left(\frac{p-1}{2}\right)!(-1)^{1+2+\cdots+\frac{(p-1)}{2}}\quad(\bmod p).$$

这给出

$$2^{\frac{(p-1)}{2}}\left(\frac{p-1}{2}\right)!\equiv\left(\frac{p-1}{2}\right)!(-1)^{\frac{(p^2-1)}{8}}\quad(\bmod p).$$

因为$\left(\frac{(p-1)}{2}\right)!\not\equiv0(\bmod p)$，这推出

$$2^{\frac{(p-1)}{2}} \equiv (-1)^{\frac{(p^2-1)}{8}} \quad (\text{mod} p).$$

根据Euler 准则，我们有$2^{\frac{(p-1)}{2}} \equiv \left(\frac{2}{p}\right) \quad (\text{mod} p)$.
因为同余式两边是 1 或-1，故二者相等. 证明完成.

9.4 Gauss引理

Euler 准则给出了计算$\left(\frac{n}{p}\right)$的一个明确的方法，但对于较大的n，计算可能变得行不通，因为这个方法需要把n自乘$\frac{(p-1)}{2}$次. Gauss发现了另一个准则，这个准则只需一个简单的计算.

定理9.6 Gauss引理. 假设$n \not\equiv 0(\text{mod} p)$. 考虑下面$\frac{(p-1)}{2}$个n的倍数

(3) $n, 2n, 3n, \cdots, \frac{p-1}{2}n$

对模P的最小正剩余. 如果m表示这些剩余中大于$\frac{P}{2}$的个数，那么

$$\left(\frac{n}{p}\right) = (-1)^m.$$

证明 (3)中各数对模p是不同余的. 我们考虑它们的最小正剩余，并根据这些最小正剩余是$<\frac{p}{2}$或是$>\frac{p}{2}$而把它们分为互不相交的两个集合A与B，如

$$A = \{a_1, a_2, \cdots, a_k\}$$

其中每一个$a_i \equiv tn \pmod{p}$，t是$\leqslant \frac{(p-1)}{2}$的某个正整数，$0 < a_i < \frac{p}{2}$.

$$B = \{b_1, b_2, \cdots, b_m\}$$

其中每个$b_i \equiv sn \pmod{P}$，s是$\leqslant \frac{(p-1)}{2}$的某个正整数，$\frac{p}{2} < b_i < p$. 注意，由于A与B是互不相交的，故有$m + k = \frac{(p-1)}{2}$. B中元素的个数就是定理中的m. 由p减去每一个b_i而得m个元素组成一个新的集合C，

$$C = \{c_1, c_2, \cdots, c_m\}, \quad c_i = p - b_i.$$

于是$0 < c_i < \frac{p}{2}$。所以C与A的元素在同一个区间内。下面我们证明集合A与C互不相交.

说对某个i与j有$c_i = a_j$，则$p - b_i = a_j$或者$a_j + b_i \equiv 0 \pmod{p}$，因此，

$$tn + sn = (t+s)n \equiv 0 \pmod{P}$$

对某个s与t成立，而且$1 \leqslant t \leqslant \frac{p}{2}$，$1 \leqslant s < \frac{p}{2}$. 但这是不可能的，因为$P \nmid n$并且$0 < s + t < P$. 因此A与C不相交，所以它们的并集$A \cup C$在区间$\left[1, \frac{(p-1)}{2}\right]$内包含有$m + k = \frac{(p-1)}{2}$个整数，于是

$$A \cup C = \{a_1, a_2, \cdots, a_k, c_1, c_2, \cdots, c_m\}$$
$$= \left\{1, 2 \cdots, \frac{p-1}{2}\right\}.$$

$A \cup C$中所有元素的乘积为

$$a_1a_2\cdots a_kc_1c_2\cdots c_m=\left(\frac{p-1}{2}\right)!\ .$$

因$c_i=p-b_i$，所以

$$\begin{aligned}\left(\frac{p-1}{2}\right)! &= a_1a_2\cdots a_k(p-b_1)(p-b_2)\cdots(p-b_m)\\ &\equiv(-1)^m a_1a_2\cdots a_kb_1b_2\cdots b_m\\ &\equiv(-1)^m n(2n)(3n)\cdots\left(\frac{p-1}{2}\right)n\\ &\equiv(-1)^m n^{\frac{(P-1)}{2}}\left(\frac{p-1}{2}\right)!\quad(\text{mod}p),\end{aligned}$$

消去阶乘，我们得

$$n^{\frac{(P-1)}{2}}\equiv(-1)^m\quad(\text{mod}p).$$

Euler准则指出$(-1)^m\equiv\left(\frac{n}{p}\right)$ (mod$p$)，于是

$(-1)=\left(\frac{n}{p}\right)$. Gauss引理的证明完成. □

在应用Gauss引理时，实际上我们不需知道m的准确的值而只需知道它的奇偶性，即m是奇数或偶数即可. 下面的定理给出一个简便的方法去确定m的奇偶性.

定理9.7　令m是Gauss引理中定义的数，则

$$m\equiv\sum_{t=1}^{\frac{P-1}{2}}\left[\frac{tn}{p}\right]+(n-1)\frac{p^2-1}{8}\quad(\text{mod}2).$$

特别，当n是奇数时，我们有

$$m\equiv\sum_{t=1}^{\frac{(P-1)}{2}}\left[\frac{tn}{p}\right]\quad(\text{mod}2).$$

证明　回忆到，m是数

$$n, 2n, 3n, \cdots, \frac{p-1}{2}n$$

的最小正剩余中大于$\frac{p}{2}$的数的个数.取一个有代表性的数，比如tn，用p去除它，并观察余数的大小，我 们有

$$\frac{tn}{p}=\left[\frac{tn}{p}\right]+\left\{\frac{tn}{p}\right\}, \text{ 其中} 0<\left\{\frac{tn}{p}\right\}<1,$$

所以，

$$tn=p\left[\frac{tn}{p}\right]+p\left\{\frac{tn}{p}\right\}=p\left[\frac{tn}{p}\right]+r_t,$$

其中$0<r_t<p$，数$r_t=tn-P\left[\frac{tn}{p}\right]$是tn对模P的最小正剩余.再一次利用在Gauss引理的证明中提到的 集合 A与B，我们有

$$\{r_1, r_2, \cdots, r_{\frac{(p-1)}{2}}\}$$
$$=\{a_1, a_2, \cdots, a_k, b_1, b_2, \cdots b_m\},$$

还回忆到

$$\left\{1, 2, \cdots, \frac{(p-1)}{2}\right\}$$
$$=\{a_1, a_2, \cdots, a_k, c_1, c_2, \cdots, c_m\},$$

其中每一个$c_i=p-b_i$. 我们计算这些集合 中元素的和，得到两个等式

$$\sum_{t=1}^{\frac{(P-1)}{2}} r_t=\sum_{i=1}^{k} a_i+\sum_{j=1}^{m} b_j.$$

与

$$\sum_{t=1}^{\frac{(P-1)}{2}} t=\sum_{i=1}^{k} a_i+\sum_{j=1}^{m} c_j=\sum_{i=1}^{k} a_i+mp-\sum_{j=1}^{m} b_j.$$

在第一个等式里，我们用r_t的定义去代替它，得到

$$\sum_{i=1}^{k} a_i + \sum_{j=1}^{m} p_j = n \sum_{t=1}^{\frac{(P-1)}{2}} t - p \sum_{t=1}^{\frac{(P-1)}{2}} \left[\frac{tn}{p}\right].$$

第二个等式就是

$$mp + \sum_{i=1}^{k} a_i - \sum_{j=1}^{m} b_j = \sum_{t=1}^{\frac{(P-1)}{2}} t.$$

把这两个式子相加，我们得

$$mp + 2\sum_{i=1}^{k} a_i = (n+1) \sum_{t=1}^{\frac{(P-1)}{2}} t - p \sum_{t=1}^{\frac{(P-1)}{2}} \left[\frac{tn}{p}\right]$$

$$= (n+1)\frac{p^2-1}{8} - p \sum_{t=1}^{\frac{(P-1)}{2}} \left[\frac{tn}{p}\right].$$

我们对模 2 来简化这个式子，注意 $n+1 \equiv n-1 \pmod 2$ 与 $P \equiv 1 \pmod 2$，我们得到

$$m \equiv (n-1)\frac{p^2-1}{8} + \sum_{t=1}^{\frac{(P-1)}{2}} \left[\frac{tn}{p}\right] \qquad \pmod 2.$$

证明完成.

9.5 二次互反律

为解决二次剩余理论里的第一个基本问题，Euler准则与Gauss引理都给出了明确的有时是冗长的步骤. 而第二个问题更困难. 它的解决依赖于一个被称为二次互反律的著名的定理，这个定理首先由Euler在1744—1746年间以一种难懂的形式表述出来，接着在1785年由Legendre重新发现这个定理并给出一部分证明. Gauss在18岁时独立地发现了互反律，并在一年后，在1796年第一个给出了它的完全的证明.

二次互反律说明，如果p与q是不同的奇素数，那么

$\left(\frac{p}{q}\right)=\left(\frac{q}{p}\right)$，除非$p\equiv q\equiv 3(\bmod 4)$)．而在$p\equiv q\equiv 3(\bmod 4)$的情况下，$\left(\frac{p}{q}\right)=-\left(\frac{q}{p}\right)$．此定理常用Legendre给出的下面的对称形式来表述．

定理9.8　二次互反律．如果p与q是不同的奇素数，那么

$$(4)\quad \left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=(-1)^{\frac{(p-1)(q-1)}{4}}.$$

证明　根据Gauss引理与定理9.7，我们有

$$\left(\frac{q}{p}\right)=(-1)^{m},$$

其中

$$m=\sum_{t=1}^{\frac{(p-1)}{2}}\left[\frac{tq}{p}\right]\quad(\bmod 2).$$

类似地，有

$$\left(\frac{p}{q}\right)=(-1)^{n},$$

其中

$$n\equiv\sum_{s=1}^{\frac{(q-1)}{2}}\left[\frac{sp}{q}\right]\quad(\bmod 2)$$

于是$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=(-1)^{m+n}$，由等式

$$(5)\quad \sum_{t=1}^{\frac{(p-1)}{2}}\left[\frac{tq}{p}\right]+\sum_{s=1}^{\frac{(q-1)}{2}}\left[\frac{sp}{q}\right]=\frac{p-1}{2}\cdot\frac{q-1}{2},$$

立即可得(4)．

为证明(5)，考虑函数

$$f(x,y)=qx-py,$$

如果x与y都是非零整数，那么$f(x,y)$也是非零整数．当x取值$1,2,\cdots,\frac{(p-1)}{2}$，y取值$1,2,\cdots,\frac{(q-1)}{2}$时，$f(x,y)$有$\frac{(p-1)}{2}\cdot\frac{(q-1)}{2}$个值，它们中任何两个不相等，因为

$$f(x,y)-f(x',y')=f(x-x',y-y')\neq 0.$$

现在我们计算$f(x,y)$的值中正值的个数与负值的个数．

对于每一个固定的x，我们有，$f(x,y)>0$当且仅当$y<\frac{qx}{p}$或者$y\leqslant\left[\frac{qx}{p}\right]$．于是，正值的总数是

$$\sum_{x=1}^{\frac{(p-1)}{2}}\left[\frac{qx}{p}\right].$$

类似地，负值的总数是

$$\sum_{y=1}^{\frac{(q-1)}{2}}\left[\frac{py}{q}\right].$$

因为正值与负值个数的总和是

$$\frac{p-1}{2}\quad\frac{q-1}{2},$$

这就证明了(5)，也就证明了(4)． □

注：读者容易看出，利用平面上的格点，有益于对(5)的证明作出几何解释．

至少发表了二次互反律的150个证明．Gauss本人至少作出了8个证明，其中包括一个直接给出的译文．二次互反律的一个更短的证明由M．Gerstenhaber[25]在一篇论文里描述过．

9.6 互反律的应用

下面的一些例子指出如何利用二次互反律去解决二次剩余理论里的两类基本问题.

例1 确定219对模383是二次剩余或二次非剩余.

解

我们利用积性、互反律、周期性以及其前面计算过的特殊值$\left(\frac{-1}{p}\right)$与$\left(\frac{2}{p}\right)$去确定符号$\left(\frac{219}{383}\right)$的值.

因为$219=3\cdot73$，由积性得

$$\left(\frac{219}{383}\right)=\left(\frac{3}{383}\right)\left(\frac{73}{383}\right).$$

利用互反律与周期性，我们有

$$\left(\frac{3}{383}\right)=\left(\frac{383}{3}\right)(-1)^{\frac{(383-1)(3-1)}{4}}=-\left(\frac{-1}{3}\right)$$

$$=-(-1)^{\frac{(3-1)}{2}}=1,$$

$$\left(\frac{73}{383}\right)=\left(\frac{383}{73}\right)(-1)^{\frac{(383-1)(73-1)}{4}}=\left(\frac{18}{73}\right)$$

$$=\left(\frac{2}{73}\right)\left(\frac{9}{73}\right)=\left(\frac{2}{73}\right)=(-1)^{\frac{(73^2-1)}{8}}=1.$$

于是$\left(\frac{218}{383}\right)=1$，所以219是模383的二次剩余.

例 2 分别确定奇素数p，使$\left(\frac{3}{p}\right)=1$及$\left(\frac{3}{p}\right)=-1$.

解

根据互反律我们有

$$\left(\frac{3}{p}\right)=\left(\frac{p}{3}\right)(-1)^{\frac{(p-1)(3-1)}{4}}$$

$$=(-1)^{\frac{(p-1)}{2}}\left(\frac{p}{3}\right).$$

为确定$\left(\frac{p}{3}\right)$，我们需要知道P的值mod3．而为确定$(-1)^{\frac{(p-1)}{2}}$，我们需要知道$\frac{(p-1)}{2}$的值mod2，或者P的值mod4．于是我们考虑Pmod12．因为P是奇素数，我们只考虑四种情形，$p\equiv1，5，7，11(\mathrm{mod}12)$，其它情形被排除．

情形1． $p\equiv1(\mathrm{mod}12)$， 此时， $p\equiv1(\mathrm{mod}3)$ 所以$\left(\frac{p}{3}\right)=\left(\frac{1}{3}\right)=1$．还有，此时$p\equiv1(\mathrm{mod}4)$， 所以$\frac{(p-1)}{2}$是偶数，于是$\left(\frac{3}{p}\right)=1$．

情形2． $p\equiv5(\mathrm{mod}12)$， 此时$p\equiv2(\mathrm{mod}3)$， 所以$\left(\frac{p}{3}\right)=\left(\frac{2}{3}\right)=(-1)^{\frac{(3^2-1)}{8}}=-1$， 还因$p\equiv1(\mathrm{mod}4)$ $\frac{(p-1)}{2}$是偶数，所以$\left(\frac{3}{p}\right)=-1$．

情形3． $p\equiv7(\mathrm{mod}12)$． 此时$p\equiv1(\mathrm{mod}3)$ 所以$\left(\frac{p}{3}\right)=\left(\frac{1}{3}\right)=1$，还因为$p\equiv3(\mathrm{mod}4)$，$\frac{(p-1)}{2}$是奇数，所以$\left(\frac{3}{p}\right)=-1$．

情形4． $p\equiv11(\mathrm{mod}12)$，此时$p\equiv2(\mathrm{mod}3)$， 所以$\left(\frac{p}{3}\right)=\left(\frac{2}{3}\right)=-1$，还因为$p\equiv3(\mathrm{mod}4)$，$\frac{(p-1)}{2}$是奇

数，于是$\left(\frac{3}{p}\right)=1$.

总结上述结果，我们得

$3Rp$　当$p\equiv\pm1 \pmod{12}$时，

$3\overline{R}p$　当$p\equiv\pm5 \pmod{12}$时.

9.7 Jacobi符号

为确定一个复合数是模p的二次剩余或二次非剩余，考虑由二次特征的因子所确定的几种情形是必要的，由于利用Jacobi引入的Legendre符号的一个推广，某些计算可以简化.

定义　如果p是一个正的奇数，具有素因子分解式

$$p=\prod_{i=1}^{r} p_i^{\alpha_i},$$

则对所有的整数n，Jacobi符号$\left(\frac{n}{p}\right)$由等式

$$(6)\quad \left(\frac{n}{p}\right)=\prod_{i=1}^{r}\left(\frac{n}{p_i}\right)^{\alpha_i}$$

确定，其$\left(\frac{n}{p_i}\right)$是Legendre符号. 我们还规定$\left(\frac{n}{1}\right)=1$.

$\left(\frac{n}{p}\right)$的可能的值为1，-1或0. 而$\left(\frac{n}{p}\right)=0$当且仅当$(n,p)>1$时.

如果同余式

$$x^2\equiv n \pmod{p}$$

有一解，那么对(6)中每一个素数p_i，都有$\left(\frac{n}{p_i}\right)=1$，于

是$\left(\frac{n}{p}\right)=1$.但是，反过来并不一定成立．因为(6)中如果出现偶数个因子-1，$\left(\frac{n}{p}\right)$能够是1.

读者能够验证下列Jacobi符号的性质，这些性质容易由Legendre符号的性质推出.

定理9.9　如果p与Q都是正奇数，我们有

(a) $\left(\frac{m}{p}\right)\left(\frac{n}{p}\right)=\left(\frac{mn}{p}\right)$,

(b) $\left(\frac{n}{p}\right)\left(\frac{n}{Q}\right)=\left(\frac{n}{pQ}\right)$,

(c) $\left(\frac{m}{p}\right)=\left(\frac{n}{p}\right)$　　当$m\equiv n \pmod{p}$时,

(d) $\left(\frac{a^2n}{p}\right)=\left(\frac{n}{p}\right)$　　当$(a,p)=1$时.

求Legendre符号$\left(\frac{-1}{p}\right)$与$\left(\frac{2}{p}\right)$的特殊公式对Jacobi符号$\left(\frac{-1}{p}\right)$与$\left(\frac{2}{p}\right)$也是正确的.

定理9.10　如果p是一个正奇数，则有

(7) $\left(\frac{-1}{p}\right)=(-1)^{\frac{(P-1)}{2}}$,

(8) $\left(\frac{2}{p}\right)=(-1)^{\frac{(P^2-1)}{8}}$.

证明　写$p=p_1p_2\cdots p_m$,其中素因子p_i不一定不同．这还可写为

$$p=\prod_{i=1}^{m}(1+p_i-1)=1+\sum_{i=1}^{m}(P_i-1)$$
$$+\sum_{i\neq j}(p_i-1)(p_j-1)+\cdots,$$

但每一个因数p_i-1是偶数，所以第一个和式后面的每一个和式都被4整除，于是

$$p \equiv 1+\sum_{i=1}^{m}(p_i-1) \pmod 4$$

或者

$$\frac{1}{2}(p-1) \equiv \sum_{i=1}^{m}\frac{1}{2}(p_i-1) \pmod 2.$$

因此

$$\left(\frac{-1}{p}\right)=\prod_{i=1}^{m}\left(\frac{-1}{p_i}\right)=\prod_{i=1}^{m}\frac{(p_i-1)}{2}=(-1)^{\frac{(p-1)}{2}}.$$

这证明了(7).

为证明(8)，我们写

$$p^2=\prod_{i=1}^{m}(1+p_i^2-1)=1+\sum_{i=1}^{m}(p_i^2-1)$$
$$+\sum_{i\neq j}(p_i^2-1)(p_j^2-1)+\cdots$$

因为p_i是奇数，所以有$p_i^2-1\equiv 0 \pmod 8$.

$$p^2\equiv 1+\sum_{i=1}^{m}(p_i^2-1) \pmod{64}.$$

于是

$$\frac{1}{8}(p^2-1)\equiv \sum_{i=1}^{m}(p_i^2-1) \pmod 8.$$

此式对模2也成立，所以

$$\left(\frac{2}{p}\right)=\prod_{i=1}^{m}\left(\frac{2}{p_i}\right)=\prod_{i=1}^{m}(-1)^{\frac{(p_i^2-1)}{8}}$$
$$=(-1)^{\frac{(p^2-1)}{8}}.$$

这证明了(8).

定理9.11 Jacobi符号的互反律.如果p与Q都是正奇

数，$(p,Q)=1$，那么，

$$(p|Q)\left(\frac{Q}{p}\right)=(-1)^{\frac{(P-1)(Q-1)}{4}}.$$

证明　写$p=p_1\cdots p_m$，$Q=q_1\cdots q_n$，其中p_i，q_i都是奇素数．于是

$$\left(\frac{p}{Q}\right)\left(\frac{Q}{p}\right)=\prod_{i=1}^{m}\prod_{j=1}^{n}\left(\frac{p_i}{q_j}\right)\left(\frac{q_j}{p_i}\right)=(-1)^r.$$

对每一个因子应用二次互反律，我们得

$$r=\sum_{i=1}^{m}\sum_{j=1}^{n}\frac{1}{2}(p_i-1)\frac{1}{2}(q_j-1)$$
$$=\sum_{j=1}^{m}\frac{1}{2}(p_i-1)\sum_{j=1}^{m}\frac{1}{2}(q_j-1).$$

在定理9.10的证明中，我们看到，

$$\sum_{i=1}^{m}\frac{1}{2}(p_i-1)\equiv\frac{1}{2}(p-1)\pmod 2.$$

对于$\sum\frac{1}{2}(q_j-1)$也能得到一个相应的同余式，因此

$$r\equiv\frac{p-1}{2}\cdot\frac{Q-1}{2}\pmod 2.$$

证明完成．

例1．　确定888是素数1999的二次剩余或二次非剩余．

解

我们有

$$\left(\frac{888}{1999}\right)=\left(\frac{4}{1999}\right)\left(\frac{2}{1999}\right)\left(\frac{111}{1999}\right)=\left(\frac{111}{1999}\right).$$

利用Legendre符号计算$\left(\frac{111}{1999}\right)$，我们写

$$\left(\frac{111}{1999}\right)=\left(\frac{3}{1999}\right)\left(\frac{37}{1999}\right).$$

并对右端每个因子应用二次互反律．而作为Jacobi符号，其计算是简单的，因为我们有

$$\left(\frac{111}{1999}\right)=-\left(\frac{1999}{111}\right)=-\left(\frac{1}{111}\right)=-1.$$

因此888是1999的二次非剩余．

例2． 确定－104是素数997的二次剩余或二次非剩余．

解

因为104＝2·4·13，我们有

$$\left(\frac{-104}{997}\right)=\left(\frac{-1}{997}\right)\left(\frac{2}{997}\right)\left(\frac{13}{997}\right)=-\left(\frac{13}{997}\right)$$

$$=-\left(\frac{997}{13}\right)=-\left(\frac{9}{13}\right)=-1,$$

因此，－104是997的二次非剩余．

9.8 对Diophantu方程的应用

亚历山大的Diophantu之后，求整数解的方程称为Diophantu方程，它的一个例子是方程

(9) $y^2=x^3+k$,

其中k是给定的整数．这个问题就是决定，对一个给定的k，方程有没有整数解x，y．如果有的话，把所有这些解表示出来．

我们讨论这个方程的部分原因是它有很长的可以追溯到十七世纪的历史，另一部分原因是某些情况可以借助于二次剩余理论来处理．一个一般的定理指出，Diophantu方程

$$y^2=f(x)$$

最多只有有限多个解，如果$f(x)$是一个次数$\geqslant 3$的具有不同的根的整系数多项式的话．[参看Le Veque [44] Vol.2里的定理4—18.]但是，除了很特殊的情形之外，没有确定这些解的方法．（甚至解的个数．）下面的定理描述(9)没有整数解的那些k值的一个无穷集合．

定理9.12　Diophantu方程

(10) $y^2=x^3+k$

没有整数解，如果k有形式

(11) $k=(4n-1)^3-4m^2$,

其中m与n是整数，使得没有素数$p\equiv -1\pmod 4$整除m.

证明　我们假设存在解x，y，并由所讨论的方程对模4得到一个矛盾．

因为$k\equiv -1\pmod 4$，所以有

(12) $y^2\equiv x^3-1\pmod 4$,

而对每一个y，$y^2\equiv 0$或$1\pmod 4$，所以当x是偶数或$x\equiv -1\pmod 4$时，(12)式不成立．因此，我们必须有$x\equiv 1\pmod 4$．于是令

$$a=4n-1,$$

所以$k=a^3-4m^2$，把(10)写为形式

(13) $y^2+4m^2=x^3+a^3=(x+a)(x^2-ax+a^2)$.

因为$x\equiv -1\pmod 4$以及$a\equiv -1\pmod 4$，我们有

(14) $x^2-ax+a^2\equiv 1-a+a^2\equiv -1\pmod 4$.

于是x^2-ax+a^2是奇数，并且(14)指出，它的所有素因子不能$\equiv 1\pmod 4$，因此有某个素数$p\equiv -1\pmod 4$整除x^2-ax+a^2，并由(13)看出，它也整除y^2+4m^2．即，

(15) $y^2\equiv -4m^2\pmod p$ 对某个$p\equiv -1\pmod 4$.

但据假设$p\nmid m$，所以$\left(-\frac{4m^2}{p}\right)=\left(-\frac{1}{p}\right)=-1$，与(15)式矛盾. 这证明了，当k有形式(11)时，Diophantu方程(10)没有整数解. □

下面的表给出适合定理9.12的k的一些值

n	0	0	0	0	1	1	1	1	2	2	2	2
m	1	2	4	5	1	2	4	5	1	2	4	5
k	−5	−17	−65	−100	23	11	−37	−73	339	327	279	243

注：当$-100\leqslant k\leqslant 100$时，(10)的所有的解已经算出．（参看[32]．）而对下列$k\leqslant 100$的正值，(10)没有整数解.

k = 6, 7, 11, 13, 14, 20, 21, 23, 29, 32, 34, 39, 42, 45, 46, 47, 51, 53, 58, 59, 60, 61, 62, 66, 67, 69, 70, 74, 75, 77, 78, 83, 84, 85, 86, 87, 88, 90, 93, 95, 96.

9.9 Gauss和与二次互反律

本节借助于Gauss和

(16) $G(n, x)=\sum_{r \bmod p} x(r)e^{\frac{2\pi i n r}{p}}$

给出二次互反律的另一个证明，其中$x(r)=\left(\frac{r}{p}\right)$是模p的二次特征. 因为模是素数，x是本原特征，因而可分性

(17) $G(n, x)=\left(\frac{n}{p}\right)G(1, x)$

对每个n成立．还有，定理8.11指出$|G(1, \chi)|^2=p$．下面的定理证明$G(1, \chi)^2$是$\pm p$．

定理9.13 如果p是一个奇素数并且$\chi(r)=\left(\frac{r}{p}\right)$，则有

(18) $$G(1, \chi)^2=\left(\frac{-1}{p}\right)p.$$

证明 我们有

$$G(1, \chi)^2=\sum_{r=1}^{p-1}\sum_{s=1}^{p-1}\left(\frac{r}{p}\right)\left(\frac{s}{p}\right)e^{\frac{2\pi i(r+s)}{p}}.$$

对每一对r，r有唯一的一个 tmodp，使得$s\equiv tr \pmod p$，且$\left(\frac{r}{p}\right)\left(\frac{s}{p}\right)=\left(\frac{r}{p}\right)\left(\frac{tr}{p}\right)=\left(\frac{r^2}{p}\right)\left(\frac{t}{p}\right)=\left(\frac{t}{p}\right)$，于是

$$\begin{aligned}G(1, \chi)^2&=\sum_{t=1}^{p-1}\sum_{r=1}^{p-1}\left(\frac{t}{p}\right)e^{\frac{2\pi i r(1+t)}{p}}\\&=\sum_{t=1}^{p-1}\left(\frac{t}{p}\right)\sum_{r=1}^{p-1}e^{\frac{2\pi i r(1+t)}{p}},\end{aligned}$$

最后的r上的和是由下式给定的几何和，

$$\sum_{r=1}^{p-1}e^{\frac{2\pi i r(1+t)}{p}}=\begin{cases}-1 & 当p\nmid(1+t)时,\\ p-1 & 当p\mid(1+t)时.\end{cases}$$

因此，

$$\begin{aligned}G(1, \chi)^2&=-\sum_{t=1}^{p-2}\left(\frac{t}{p}\right)+(p-1)\left(\frac{p-1}{p}\right)\\&=-\sum_{t=1}^{p-1}\left(\frac{t}{p}\right)+p\left(\frac{-1}{p}\right)\\&=\left(\frac{-1}{p}\right)p,\end{aligned}$$

这因为$\sum_{t=1}^{p-1}\left(\frac{t}{p}\right)=0$．(18)得证． ∎

等式(18)指出$G(1, \chi)^2$是一个整数，所以对每一个奇

数q，$G(1, x)^{q-1}$也是一个整数．下面的定理证明，二次互反律与这些整数的值modq有联系．

定理9.14　令p与q是不同的奇素数，并令x是模p的二次特征，那么二次互反律

$$(19)\quad \left(\frac{q}{p}\right)=(-1)^{\frac{(p-1)(q-1)}{4}}\left(\frac{p}{q}\right)$$

等价于同余式

$$(20)\quad G(1, x)^{q-1}\equiv\left(\frac{q}{p}\right)\pmod q.$$

证明　由(18)我们有

$$(21)\quad G(1, x)^{q-1}=\left(-\frac{1}{p}\right)^{\frac{(q-1)}{2}}p^{\frac{(q-1)}{2}}$$

$$=(-1)^{\frac{(p-1)(q-1)}{4}}p^{\frac{(q-1)}{2}}.$$

根据Euler准则，我们有$p^{\frac{(q-1)}{2}}\equiv\left(\frac{p}{q}\right)\pmod q$，

所以(21)推出

$$(22)\quad G(1, x)^{q-1}\equiv(-1)^{\frac{(p-1)(q-1)}{4}}\left(\frac{p}{q}\right)\pmod q.$$

如果(20)成立，我们得

$$\left(\frac{q}{p}\right)\equiv(-1)^{\frac{(p-1)(q-1)}{4}}\left(\frac{p}{q}\right)\pmod q,$$

因为两边都是±1，这就推出(19)．反之，如果(19)成立，那么由(22)推出(20)．□

下面的定理给出一个等式，我们能利用它去推出(20)．

定理9.15　如果p与q是不同的奇素数，x是模p的二次特征，那么我们有

$$(23)\quad G(1,\ x)^{q-1}=\left(\frac{q}{p}\right)\sum_{\substack{r_1 \bmod p\\ r_1+\cdots+r_q\equiv q\,(\bmod p)}}\cdots\sum_{r_q \bmod p}\left(\frac{r_1\cdots r_q}{p}\right).$$

证明　Gauss和$G(n,\ x)$是n的周期函数，其周期为p。这对$G(n,\ x)^q$也是真的，所以我们有一个有限Fourier展式

$$G(n,\ x)^q=\sum_{m \bmod p}a_q(m)e^{\frac{2\pi imn}{p}},$$

其系数由

$$(24)\quad a_q(m)=\frac{1}{p}\sum_{n \bmod p}G(n,\ x)^q e^{\frac{-2\pi imn}{p}}$$

给出．由$G(n,\ x)$的定义，我们有

$$G(n,\ x)^q=\sum_{r_1 \bmod p}\left(\frac{r_1}{p}\right)e^{\frac{2\pi inr_1}{p}}\cdots\sum_{r_2 \bmod p}\left(\frac{r_q}{p}\right)e^{\frac{2\pi inr_q}{p}}$$

$$=\sum_{r_1 \bmod p}\cdots\sum_{r_q \bmod p}\left(\frac{r_1\cdots r_q}{p}\right)\times e^{\frac{2\pi in(r_1+\cdots+r_q)}{p}}$$

所以(24)变为

$$a_q(m)=\frac{1}{p}\sum_{r_1 \bmod p}\cdots\sum_{r_q \bmod p}\left(\frac{r_1\cdots r_q}{p}\right)\times\sum_{n \bmod p}e^{\frac{2\pi in(r_1+\cdots+r_q-m)}{p}}$$

n上的和是一个几何和，在$r_1+\cdots+r_q\equiv m\ (\bmod p)$时，这个几何和等于$p$，在其它情况下，这个几何和为0，于是，

$$(25)\quad a_q(m)=\sum_{\substack{r_1 \bmod p\\ r_1+\cdots+r_q\equiv m\,(\bmod p)}}\cdots\sum_{r_q \bmod p}\left(\frac{r_1\cdots r_q}{p}\right).$$

现在我们回到(24)并得到$a_q(m)$的一个替换式．利用$G(n,x)$

的可分性与$\left(\frac{n}{p}\right)^q=\left(\frac{n}{p}\right)$对奇数q成立，我们得

$$\begin{aligned}a_q(m)&=\frac{1}{p}G(1,\ x)^q\sum_{n\ \mathrm{mod}\ p}\left(\frac{n}{p}\right)e^{\frac{-2\pi imn}{p}}\\&=\frac{1}{p}G(1,\ x)^qG(-m,\ x)\\&=\frac{1}{p}G(1,\ x)^q\left(\frac{m}{p}\right)G(-1,\ x)\\&=\left(\frac{m}{p}\right)G(1,\ x)^{q-1}\end{aligned}$$

因为$G(1,\ x)G(-1,\ x)=G(1,\ x)\overline{G(1,\ x)}$

$$=|G(1,\ x)|^2=p.$$

即$G(1,\ x)^{q-1}=\left(\frac{m}{p}\right)a_q(m)$. 取$m=q$并利用(25)我们得到(23). □

互反律的证明. 为了由(23)推出互反律，只要能证明

$$(26)\quad \sum_{r_1\ \mathrm{mod}\ p}\cdots\sum_{r_q\ \mathrm{mod}\ p}\left(\frac{r_1+\cdots+r_q}{p}\right)\equiv 1\quad(\mathrm{mod}\ p)$$

就够了，其中r_1，…，r_q的总和适合条件

$$(27)\quad r_1+\cdots+r_q\equiv q\quad(\mathrm{mod}\ p).$$

如果r_1，…，r_q中每一个都与其它的同余modp，那么，它们的和同余于qr_j，$j=1, 2, \cdots, q$. 所以(27)成立当且仅当

$$qr_j\equiv q\quad(\mathrm{mod}\ p),$$

即当且仅当$r_j\equiv 1\ (\mathrm{mod}\ p)$对每个j. 此时，(26)的总和是$\left(\frac{1}{p}\right)\equiv 1\quad(\mathrm{mod}\ p)$. 对满足(27)的所有其余挑选的指标$r_1$，…，$r_q$中，一定至少有两个不同余，因此(27)的每一个

循环置换给出(27)的一个新的解，它给出相同的加数$\left(\frac{r_1 \cdots r_q}{p}\right)$. 因此，每一个这样的加数出现q次并且这个和同余于0 modp. 于是(26)里的和仅当$\left(\frac{1}{p}\right)=1$时不为0 modp，这就完成了证明. □

9.10 二次Gauss和的互反律

本节讨论二次互反律的另一个证明，它是在二次高斯和

$$(28)\quad G(n;\ m)=\sum_{r=1}^{m} e^{\frac{2\pi i n r^2}{m}}$$

的基础上进行的. 如果p是一个奇素数，p∤n，则有

$$(29)\quad G(n;\ p)=\left(\frac{n}{p}\right)G(1;\ p).$$

它把和G(n; p)的研究简化为研究n=1的情形. 等式(29)容易由(28)得到或根据注释G(n; p)=G(n, x)得出，其中$x(n)=\left(\frac{n}{p}\right)$，注意G(n, x)是可分的.

虽然和G(1; p)的每一项绝对值为1，而G(1; p)本身的绝对值为0，$\sqrt{p}$或$\sqrt{2p}$. 特别，Gauss证明了重要公式

$$(30)\quad G(1;\ m)=\frac{1}{2}\sqrt{m}\,(1+i)(1+e^{-\frac{\pi i m}{2}})$$

$$=\begin{cases}\sqrt{m} & m\equiv 1\ (\bmod 4)\\ 0 & m\equiv 2\ (\bmod 4)\\ i\sqrt{m} & m\equiv 3\ (\bmod 4)\\ (1+i)\sqrt{m} & m\equiv 0\ (\bmod 4)\end{cases}$$

对每一个m≥1成立. (30)的不同证明的个数是众所周知的.

我们将讨论一个有关的和

$$S(a,\ m)=\sum_{r=0}^{m-1} e^{\frac{\pi i a r^2}{m}}$$

来推出(30)，其中a与m是正整数．若$a=2$，则$S(2,\ m)=G(1;\ m)$．

和$S(a,\ m)$也有个互反律（表述在下面的定理9.16中，它推出Gauss和公式(30)并且还引出二次互反律的另一个证明．

定理9.16　如果乘积ma是偶数，那么我们有

$$(31)\quad S(a,\ m)=\sqrt{\frac{m}{a}}\left(\frac{1+i}{\sqrt{2}}\right)\overline{S(m,\ a)}$$

其中横线表示复数的共轭．

注意　为推出Gauss和公式(30)我们在(31)里取$a=2$并注意$\overline{S(m,\ 2)}=1+e^{\frac{-\pi i m}{2}}$．

证明　此证明是在残数计算的基础上进行的．令g是由等式

$$(32)\quad g(z)=\sum_{r=0}^{m-1} e^{\frac{\pi i a (z+r)^2}{m}}$$

定义的函数，则g是处处解析的，并且$g(0)=S(a,\ m)$．因为ma是偶数，我们看出

$$g(z+1)-g(z)=e^{\frac{\pi i a z^2}{m}}(e^{2\pi i a z}-1)$$

$$=e^{\frac{\pi i a z^2}{m}}(e^{2\pi i z}-1)\sum_{n=0}^{a-1} e^{2\pi i n z}.$$

现在由等式

$$f(z)=\frac{g(z)}{e^{2\pi i z}-1}$$

定义f，则f除开每个整数为一级级点外处处解析，并且f满足等式

$$(33)\quad f(z+1)=f(z)+\varphi(z),$$

其中

$$(34)\quad \varphi(z)=e^{\frac{\pi i a z^2}{m}}\sum_{n=0}^{a-1}e^{2\pi i n z}$$

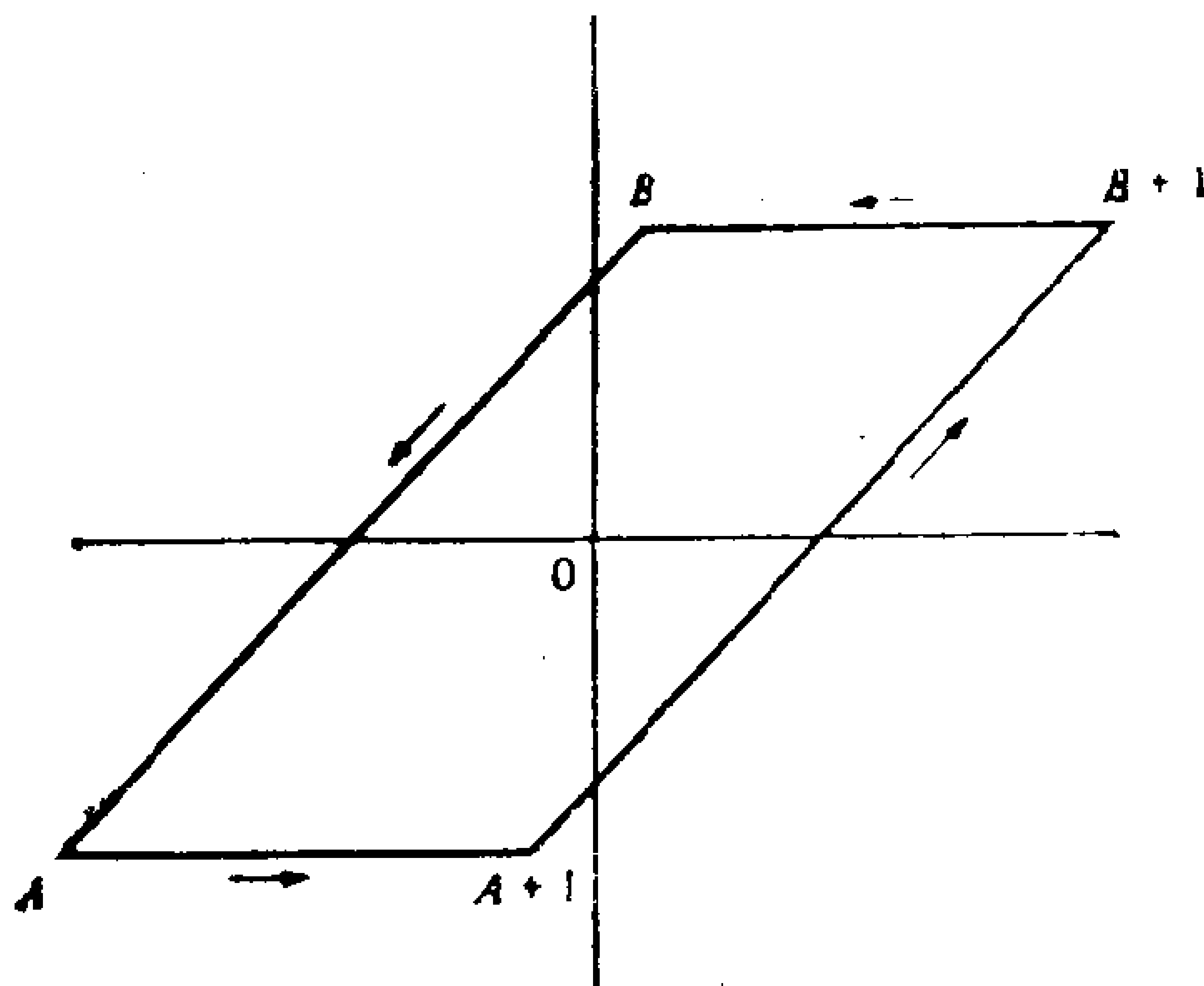
是处处解析的．

在$z=0$时，f的残数是$\frac{g(0)}{(2\pi i)}$，于是

$$(35)\quad S(a,\ m)=g(0)=2\pi i\operatorname*{Res}_{z=0}f(z)=\int_{r}f(z)dz,$$

其中r是一个正向纵标的简单封闭线路，它的图形内部区域只含极点$z=0$．我们选择r，使它描绘出一个以A，$A+1$，$B+1$，B为顶点的平行四边形，其中

$$A=-\frac{1}{2}-Re^{\frac{\pi i}{4}}\qquad B=-\frac{1}{2}+Re^{\frac{\pi i}{4}}$$



（图9.1）

如图9.1所示．f沿r积分，我们有

$$\int_r f=\int_A^{A+1} f+\int_{A-1}^{B+1} f+\int_{B+1}^{B} f+\int_B^A f.$$

在积分$\int_{A+1}^{B+1} f$里，我们作变量替换$W=z+1$，并利用(33)得

$$\int_{A+1}^{B+1} f(w)dw=\int_A^B f(z+1)dz$$

$$=\int_A^B f(z)dz+\int_A^B \varphi(z)dz.$$

因此，(35)变为

$$(36)\quad S(a,\ m)=\int_A^B \varphi(z)dz+\int_A^{A+1} f(z)dz$$

$$-\int_B^{B+1} f(z)dz.$$

现在我们证明，当$R\to\infty$时，沿着A到A+1与沿着由B到B+1的水平线段的积分趋于0．为此，我们估算这两个水平线段上的积分，我们写

$$(37)\quad |f(z)|=\frac{|g(z)|}{|e^{2\pi iz}-1|},$$

并分别计算其分子与分母．

在联结B到B+1的水平线段上，我们令

$$r(t)=t+Re^{\frac{\pi i}{4}}\quad 其中-\frac{1}{2}\leqslant t\leqslant\frac{1}{2}.$$

由(32)我们看出

$$(38)\quad |g[r(t)]|\leqslant\sum_{r=0}^{m-1}\left|\exp\left\{\frac{\pi ia(t+Re^{\frac{\pi i}{4}}+r)^2}{m}\right\}\right|,$$

其中$\exp z=e^z$．大括号内式子的实部为

$$\frac{-\pi a(\sqrt{2}tR+R^2+\sqrt{2}rR)}{m}.$$

因为 $|e^{x+iy}| = e^x$ 且 $\exp\left\{\frac{-\pi a\sqrt{2}\,rR}{m}\right\}\leqslant 1$，所以(38)式中每一项的绝对值不超过 $\exp\left\{\frac{-\pi aR^2}{m}\right\}\exp\left\{\frac{-\sqrt{2}\,\pi atR}{m}\right\}$. 但是 $-\frac{1}{2}\leqslant t\leqslant\frac{1}{2}$，所以我们得到估算式

$$|g[r(t)]|\leqslant m e^{\frac{\pi\sqrt{2}\,aR}{(2m)}} e^{\frac{-\pi aR^2}{m}}.$$

对(37)中的分子，我们利用形式为

$$|e^{2\pi iz}-1|\geqslant||e^{2\pi iz}|-1|$$

的三角不等式. 因为 $|\exp\{2\pi ir(t)\}|=\exp\left\{-2\pi R\sin\left(\frac{\pi}{4}\right)\right\}=\exp\{-\sqrt{2}\,\pi R\}$，我们得

$$|e^{2\pi ir(t)}-1|\geqslant 1-e^{-\sqrt{2}\pi R}.$$

因此，在连结B到B+1的水平线段上，我们有

$$|f(z)|\leqslant\frac{m e^{\frac{\pi\sqrt{2}\,aR}{(2m)}} e^{\frac{-\pi aR^2}{m}}}{1-e^{-\sqrt{2}\,\pi R}}=0(1)$$

当 $x\to\infty$ 时.

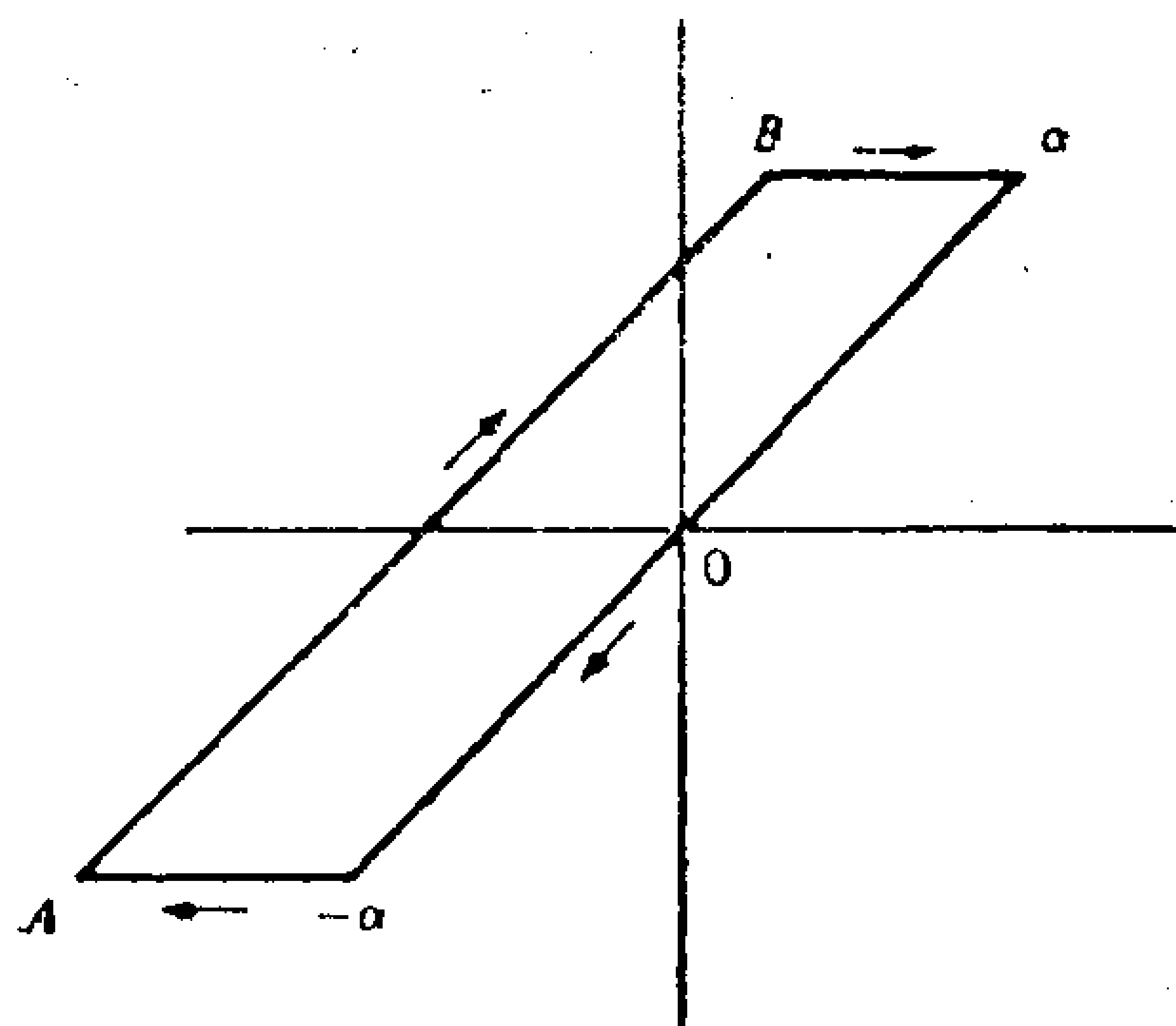
类似的理由可以证明，当 $R\to\infty$ 时，连结A到A+1的水平线段上的积分趋于0. 因为在每一种情形，积分路线的长度都是1，这说明，当 $R\to\infty$ 时，(36)右端的第二与第三个积分趋于0，因此，我们可把(36)写为

(39) $S(a,m)=\int_A^B\varphi(z)dz+0(1)$ 当 $x\to\infty$ 时.

为讨论积分 $\int_A^B\varphi$，我们应用Cauchy定理. 被积函数 φ 绕过具有顶点A，B，α，$-\alpha$ 的平行四边形，其中 $\alpha=\beta+\frac{1}{2}=Re^{\frac{\pi i}{4}}$.（图9.2）因为 φ 是处处解析的，它沿这个平行四

边形的积分为0，所以

$$(40)\quad \int_A^B \varphi + \int_B^\alpha \varphi + \int_\alpha^{-\alpha} \varphi + \int_{-\alpha}^A \varphi = 0.$$



（图9.2）

因为在(34)里指数因子是$e^{\frac{\pi i a z^2}{m}}$，同上面证明中给出的理由类似，当R→∞时，φ沿水平线段的积分→0. 因此(40)给出

$$\int_A^B \varphi = \int_{-\alpha}^{\alpha} \varphi + 0(1)$$

当R→∞时.

并且(39)变为

$$(41)\quad S(a, m) = \int_{-\alpha}^{\alpha} \varphi(z) dz + 0(1) \quad \text{当} R \to \infty \text{时},$$

其中$\alpha = Re^{\frac{\pi i}{4}}$. 利用(34)我们得到

$$\int_{-\alpha}^{\alpha} \varphi(z) dz = \sum_{n=0}^{a-1} \int_{-\alpha}^{\alpha} e^{\frac{\pi i a z^2}{m}} e^{2\pi i n z} dz$$

$$= \sum_{n=0}^{a-1} e^{\frac{-\pi i m n^2}{a}} I(a, m, n, R),$$

其中

$$I(a, m, n, R) = \int_{-\alpha}^{\alpha} \exp\left\{\frac{\pi i a}{m}\left(z + \frac{nm}{a}\right)^2\right\} dz.$$

再一次对顶点为$-\alpha$，α，$\alpha - \left(\frac{nm}{a}\right)$与$-\alpha - \left(\frac{nm}{a}\right)$的平行四边形应用Cauchy定理. 同前面一样，当R→∞时，我们得到，沿水平线段的积分→0，所以

$$I(a,n,m,R)=\int_{\frac{-\alpha-nm}{a}}^{\frac{\alpha-nm}{a}} \exp\left\{\frac{\pi ia}{m}\left(z+\frac{nm}{a}\right)^2\right\}dz$$
$$+0(1)$$

当 $R\to\infty$ 时.

变量替换 $W=\sqrt{\frac{a}{m}}\left(z+\frac{nm}{a}\right)$ 代入上式为

$$I(a,n,m,R)=\sqrt{\frac{m}{n}}\int_{-\alpha\sqrt{\frac{a}{m}}}^{\alpha\sqrt{\frac{a}{m}}} e^{\pi iw^2}\,dw+0(1)$$

当 $x\to\infty$ 时。

在(41)里令 $R\to\infty$，我们得到

$$(42)\quad S(a,\ m)=\sum_{n=0}^{a-1} e^{\frac{-\pi imn^2}{a}}\sqrt{\frac{m}{a}}$$
$$\lim_{R\to+\infty}\int_{-R\sqrt{\frac{a}{m}}\,e^{\frac{\pi i}{4}}}^{R\sqrt{\frac{a}{m}}\,e^{\frac{\pi i}{4}}} e^{\pi iw^2}\,dw$$

记 $T=\sqrt{\frac{a}{m}}\ R$，(42)中最后的极限等于

$$\lim_{T\to+\infty}\int_{-Te^{\frac{\pi i}{4}}}^{Te^{\frac{\pi i}{4}}} e^{\pi iw^2}\,dw=I,$$

其中I是与α，m无关的一个数，因此(42)给出

$$(43)\quad S(a,\ m)=\sqrt{\frac{m}{a}}\ I\overline{S(m,\ a)}.$$

为求I的值，在(43)里，我们取$a=1$，$m=2$. 于是 $S(1,\ 2)=1+i$，$S(2,\ 1)=1$，所以(43)推出$I=(1+i)\sqrt{2}$ 并且(43)推出(31). □

定理9.16推出二次Gauss和的一个互反律.

定理9.17 如果h>0，k>0，h为奇数，则

$$(44)\quad G(h;\ k)=\sqrt{\frac{k}{h}}\ \frac{1+i}{2}\left(1+e^{\frac{-\pi ihk}{2}}\right)\overline{G(k;h)}.$$

证明 在定理9.16里取$a=2h$，$m=k$，得

$$(45)\quad G(h;\ k)=S(2h,\ k)=\sqrt{\frac{k}{2h}}\ \frac{1+i}{2}\overline{S(k,\ 2h)}$$

$$=\sqrt{\frac{k}{h}}\ \frac{1+i}{2}\sum_{r=0}^{2h-1}e^{-\frac{\pi ikr^2}{(2h)}}.$$

与r为偶数、奇数相对应，我们把r上的这个和分为两部分．对于偶数r，我们写$r=2s$，$s=0,\ 1,\cdots,h-1$．对于奇数r，我们注意到$(r+2h)^2\equiv r^2\pmod{4h}$，所以这个和能在模2h的任一完全剩余系里的奇数上展开．我们计算在区间$h\leqslant r<3h$里的所有奇数上的总和，写$r=2s+h$，其中$s=0,1,2,\cdots,h-1$．（$2s+h$各数都是奇数并且对模2h互不同余．）这给出

$$\sum_{r=0}^{2h-1}e^{\frac{-\pi ikr^2}{(2h)}}=\sum_{s=0}^{h-1}e^{\frac{-\pi ik(2s)^2}{(2h)}}+\sum_{s=0}^{h-1}e^{\frac{-\pi ik(2s+h)^2}{(2h)}}$$

$$=\sum_{s=0}^{h-1}e^{\frac{-2\pi iks^2}{h}}\left(1+e^{\frac{-\pi ihk}{2}}\right)$$

$$=\left(1+e^{\frac{-\pi ihk}{2}}\right)\overline{G(k;\ h)}.$$

在(45)里利用此式即得(44)． □

9.11 二次互反律的另一个证明

Gauss公式(30)引出二次互反律的一个简捷的证明．

首先，我们注意，当k是奇数时，由(30)推出

$$G(1;k)=i^{\frac{(k-1)^2}{4}}\sqrt{K},$$

并且，我们有乘法性质（习题8.16(a)）

$$G(m;n)G(n;m)=G(1;mn)\quad 若(m,n)=1.$$

因此当p与q为不同的奇素数时，我们有

$$G(p;q)=\left(\frac{p}{q}\right)G(1;q)=\left(\frac{p}{q}\right)i^{\frac{(q-1)^2}{4}}\sqrt{q}$$

$$G(p;p)=\left(\frac{q}{p}\right)G(1;p)=\left(\frac{q}{p}\right)i^{\frac{(p-1)^2}{4}}\sqrt{p}$$

与

$$G(p;q)G(q;p)=G(1;pq)=i^{\frac{(pq-1)^2}{4}}\sqrt{pq}.$$

最后一个等式与前面两个等式比较，我们得

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)i^{\frac{((q-1)^2+(p-1^2))}{4}}=i^{\frac{(pq-1)^2}{4}},$$

由于

$$i^{\frac{((pq-1)^2-(q-1)^2-(p-1)^2)}{4}}=(-1)^{\frac{(p-1)(q-1)}{4}},$$

立即可得二次互反律。 □

第九章习题

1．确定哪些奇 素数p，有$\left(-\frac{3}{p}\right)=1$？哪些 奇素p，有$\left(-\frac{3}{p}\right)=-1$.

2．证明，如果奇素$p\equiv\pm1(\text{mod}10)$，则5是p的二次剩余；如果$p\equiv\pm3(\text{mod}10)$，则 5 是p的二次非剩余.

3. 令p是一个奇素数，设集合{1，2，…，p－1}能分为两个非空子集S与T的并，S≠T，使得同一个子集合中任意二元之积modp位于S内，而S中任一元素与T中任一元素之积modp位于T内．证明，S由模p的二次剩余组成，T由模p的二次非剩余组成．

4. 令f(x)是一个多项式，当x是整数时，f(x)取整数值．

(a) 如果a与b都是整数，证明

$$\sum_{x \bmod p}\left(\frac{f(ax+b)}{p}\right)=\sum_{x \bmod p}\left(\frac{f(x)}{p}\right)$$

当(a、p)＝1时．

并且

$$\sum_{x \bmod p}\left(\frac{af(x)}{p}\right)=\left(\frac{a}{p}\right)\sum_{x \bmod p}\left(\frac{f(x)}{p}\right)$$对所有的a．

(b) 证明，当(a，p)＝1时，

$$\sum_{x \bmod p}\left(\frac{ax+b}{p}\right)=0.$$

(c) 令f(x)＝x(ax＋b)，其中(a，p)＝(b，p)＝1，证明

$$\sum_{x=1}^{p-1}\left(\frac{f(x)}{p}\right)=\sum_{x=1}^{p-1}\left(\frac{ax+b}{p}\right)=-\left(\frac{a}{p}\right).$$

[提示：如果x过模p的一个简化剩余系，那么x的倒数x′modp也过模p的一个简化剩余系．]

5. 令α与β是可能值为±1的整数，N(α，β)是1，α，…，p－2中满足$\left(\frac{x}{p}\right)=\alpha$与$\left(\frac{x+1}{p}\right)=\beta$的x的个数，其中p是奇素数．证明

$$4N(\alpha,\beta)=\sum_{x=1}^{p-2}\left\{1+\alpha\left(\frac{x}{p}\right)\right\}\left\{1+\beta\left(\frac{x+1}{p}\right)\right\},$$

并利用第 4 题推导出

$$4N(\alpha, \beta)=p-2-\beta-\alpha\beta-\alpha\left(\frac{-1}{p}\right).$$

特别，这给出

$$N(1, 1)=\frac{p-4-\left(\frac{-1}{p}\right)}{4},$$

$$N(-1, -1)=N(-1, 1)=\frac{p-2+\left(\frac{-1}{p}\right)}{4}$$

$$N(1, -1)=1+N(1, 1).$$

6. 利用第 5 题证明，对任意素数p，存在整数x与y，使得

$$x^2+y^2+1\equiv 0 \pmod{p}.$$

7. 令p是一个奇素数，证明下列各条

(a) 当$p\equiv 1 \pmod 4$时，$\sum_{r=1}^{p-1} r\left(\frac{r}{p}\right)=0$；

(b) 当$p\equiv 1 \pmod 4$时，$\sum_{r=1}^{p-1} r=\frac{p(p-1)}{4}$；

(c) 当$p\equiv 3 \pmod 4$时，$\sum_{r=1}^{p-1} r^2\left(\frac{r}{p}\right)=p\sum_{r=1}^{p-1} r\left(\frac{r}{p}\right)$；

(d) 当$p\equiv 1 \pmod 4$时，$\sum_{r=1}^{p-1} r^3\left(\frac{r}{p}\right)=\frac{3}{2}p\sum_{r=1}^{p-1} r^2\left(\frac{r}{p}\right)$；

(e) 当$p\equiv 3 \pmod 4$时，

$$\sum_{r=1}^{p-1} r^4\left(\frac{r}{p}\right)=2p\sum_{r=1}^{p-1} r^3\left(\frac{r}{p}\right)-p^2\sum_{r=1}^{p-1} r^2\left(\frac{r}{p}\right).$$

[提示：$p-r$随着r一起通过数1，2，…，$p-1$.]

8. 令p是一个奇素数，$p\equiv 3 \pmod 4$，并令$q=\frac{(p-1)}{2}$，

(a) 证明

$$\left\{1-2\left(\frac{2}{p}\right)\right\}\sum_{r=1}^{q} r\left(\frac{r}{p}\right)=p\frac{1-\left(\frac{2}{p}\right)}{2}\sum_{r=1}^{q}\left(\frac{r}{p}\right).$$

[提示：当r通过数1，2，…，q时，r与p−r一起通过数1，2，…，p−1，同理，2r与p−2r也同样.]

(b) 证明

$$\left\{\left(\frac{2}{p}\right)-2\right\}\sum_{r=1}^{p-1} r\left(\frac{r}{p}\right)=p\sum_{r=1}^{q}\left(\frac{r}{p}\right).$$

9. 如果p是一个奇素数，令$x(n)=\left(\frac{n}{p}\right)$. 证明，当(n, p)=1时，与x相伴的Gauss和G(n, x)等于习题8.16中介绍的二次高斯和G(n; p). 即，如果n∤n，则有

$$G(n,\ x)=\sum_{m \bmod p} x(m)e^{\frac{2\pi imn}{p}}=\sum_{r=1}^{p} e^{\frac{2\pi inr^2}{p}}$$
$$=G(n;\ p).$$

应当指出，当p|n时，G(n, x)≠G(n; p). 因为此时G(p, x)=0而G(p; p)=p.

10. 利用一个互反律计算二次Gauss和G(2; p)的值.将此结果与公式$G(2;\ p)=\left(\frac{2}{p}\right)G(1;\ p)$比较，并推出，当p是一个奇素数时，$\left(\frac{2}{p}\right)=(-1)^{\frac{(p^2-1)}{8}}$.

第十章 原 根

10.1 数的次数modm、原根

令a与m是互素的整数，$m\geqslant1$. 考虑a的所有正的方幂

$$a,\ a^2,\ a^3,\ \cdots.$$

由Euler—Fermat定理，我们知道$a^{\varphi(m)}\equiv1(\mathrm{mod}\,m)$. 可能有更小的方幂$a^f$，使$a^f\equiv1(\mathrm{mod}\,m)$. 我们感兴趣的是具有此性质的最小的正整数f.

定义 满足$a^f\equiv1(\mathrm{mod}\,m)$的最小正整数f称为a的次数modm，并记为

$$f=\exp_m(a).$$

如果$\exp_m(a)=\varphi(m)$，则a叫做是模m的一个原根. Euler-Fermat定理告诉我们，$\exp_m(a)\leqslant\varphi(m)$. 下面的定理证明$\exp_m(a)$整除$\varphi(m)$.

定理10.1 **给定$m\geqslant1$，$(a,m)=1$，令$f=\exp_m(a)$. 那么我们有**

(a) $a^k\equiv a^h(\mathrm{mod}\,m)$当且仅当$k\equiv h(\mathrm{mod}\,f)$.

(b) $a^k\equiv1(\mathrm{mod}\,m)$当且仅当$k=0(\mathrm{mod}\,f)$特别，$f\mid\varphi(m)$.

(c) $1,\ a,\ a^2,\ \cdots,\ a^{f-1}$各数对模m互不同余.

证明 (b)与(c)可由(a)立即得出，所以我们只需证明

(a). 如果$a^k \equiv a^h \pmod{m}$，则$a^{k-h} \equiv 1 \pmod{m}$. 可以写

$$k-h=qf+r \quad 其中0 \leqslant r < f.$$

于是$1 \equiv a^{k-h} = a^{qf+r} \equiv a^r \pmod{m}$，所以$r=0$，$k \equiv h \pmod{f}$.

反之，如果$k \equiv h \pmod{f}$，则$k-h=qf$，所以$a^{k-h} \equiv 1 \pmod{m}$，于是$a^k \equiv a^h \pmod{m}$.

10.2 原根与简化剩余系

定理10.2 令$(a, m)=1$，则a是模m的一个原根当且仅当

(1) $a, a^2, \cdots, a^{\varphi(m)}$

成为模m的一个简化剩余系.

证明 如果a是一个原根，则根据定理10.1(c)，(1)中各数对模m互不同余. 因为这样的数有$\varphi(m)$个，所以它们形成模m的一个简化剩余系.

反之，如果(1)中各数成为一个简化剩余系，那么$a^{\varphi(m)} \equiv 1 \pmod{m}$而没有更小的方幂同余于1，所以$a$是一个原根.

注意 在第六章里，我们得到，模m的所有简化剩余类形成一个群。如果m有原根，定理10.2指出，这个群是由剩余类$\hat{a}$生成的循环群。

原根的重要性已由定理10.2阐明. 如果m有原根，那么模m的每一个简化剩余系能表为一个几何级数. 这给一个有力的工具，它在含有简化剩余系的问题中能被利用. 遗憾的是，不是所有的模都有原根. 下面几节我们将证明，只有下列的模

$$m=1, 2, 4, p^{\alpha}与2p$$

原根方存在，其中p是奇素数，$\alpha\geq 1$.

前三种情形容易确定．情形$m=1$是平凡的．对于$m=2$，数 1 是一个原根．对$m=4$，我们有$\varphi(4)=2$与$3^2\equiv 1(\mathrm{mod}4)$，所以 3 是一个原根．下面我们证明，当$\alpha\geq 3$时，模$2^\alpha$没有原根．

10.3　对$\alpha\geq 3$，模2^α的原根不存在

定理10.3　令x是一个奇数，当$\alpha\geq 3$时，我们有

$$(2)\quad x^{\frac{\varphi(2^\alpha)}{2}}\equiv 1\pmod{2^\alpha}.$$

所以，模2^α没有原根．

证明　当$\alpha=3$时，同余式(2)就是说，对奇数x，$x^2\equiv 1(\mathrm{mod}8)$．用x为1，3，5，7容易验证(2)是成立的，或者根据

$$(2k+1)^2=4k^2+4k+1=4k(k+1)+1$$

也得$x^2\equiv 1(\mathrm{mod}8)$，注意$k(k+1)$是偶数．

下面我们对α作归纳法来证明此定理．我们假设(2)对α成立并证明(2)对$\alpha+1$也成立．归纳法假设就是

$$x^{\frac{\varphi(2^\alpha)}{2}}=1+2^\alpha t,$$

其中t是整数．两边平方，得

$$x^{\varphi(2^\alpha)}=1+2^{\alpha+1}t+2^{2\alpha}t^2\equiv 1(\mathrm{mod}2^{\alpha+1}),$$

这因此$2\alpha\geq\alpha+1$．因为$\varphi(2^\alpha)=2^{\alpha-1}=\frac{\varphi(2^{\alpha+1})}{2}$，所以证明完成．

10.4 对奇素数p，模p的原根存在

首先，我们证明下面的引理.

引理1 已知$(a, m)=1$，令$f=\exp_m(a)$，则有

$$\exp_m(a^k)=\frac{\exp_m(a)}{(k, f)}.$$

特别，$\exp_m(a^k)=\exp_m(a)$当且仅当$(k, f)=1$.

证明 a^k的次数是使

$$a^{xk}\equiv 1(\bmod m)$$

的最小正整数x，也就是最小的$x>0$，使得$kx\equiv 0(\bmod f)$.而后一个同余式等价于同余式

$$x\equiv 0\left(\bmod \frac{f}{d}\right),$$

其中$d=(k, f)$. 这个同余式的最小正整数解是$\frac{f}{d}$，所以

$\exp_m(a^k)=\frac{f}{d}$，与结论相符. □

引理1可用于证明素数模的原根的存在性. 实际上，我们能确定模p的原根的准确个数.

定理10.4 **令p是一个奇素数并令d是$p-1$的任一正约数，则在模p的每一个简化剩余系里，恰有$\varphi(d)$个a使得**

$$\exp_p(a)=d.$$

特别，当$d=\varphi(p)=p-1$时，模p恰有$\varphi(p-1)$个原根.

证明 我们利用在第二章里使用过证明

$$\sum_{d\mid n}\varphi(d)=n$$

的方法，把数1，2，…，$p-1$分为互不相交的一些集合

$A(d)$，每一个集合对应着$p-1$的一个约数d，我们定义

$$A(d)=\{x:1\leqslant x<p-1\text{且}\exp_p(x)=d\}.$$

令$f(d)$是$A(d)$里元素的个数，那么，对每一个d，$f(d)\geqslant 0$，我们的目的是证明$f(d)=\varphi(d)$.

因为集合$A(d)$是互不相交的并因每一个$x=1, 2, \cdots, p-1$必属于某个$A(d)$，所以有

$$\sum_{d\mid p-1} f(d)=p-1,$$

但我们还有

$$\sum_{d\mid p-1} \varphi(d)=p-1,$$

所以

$$\sum_{d\mid p-1} \{\varphi(d)-f(d)\}=0.$$

为了证明和中每一项均为0，只要能证明$f(d)\leqslant\varphi(d)$就够了．我们证明，要么$f(d)=0$，要么$f(d)=\varphi(d)$．换言之，由$f(d)\neq 0$，必得出$f(d)=\varphi(d)$.

假设$f(d)\neq 0$，那么$A(d)$非空，所以有某个$a\in A(d)$，因此

$$\exp_p(a)=d \qquad \text{这里} a^d\equiv 1(\mathrm{mod}\,p).$$

但a的任一方幂都满足此式，所以d个数

(3) $a, a^2, \cdots, a^d$

都是同余式

(4) $x^d-1\equiv 0(\mathrm{mod}\,p)$

的解．但(4)的模是素数，它最多只有d个解，所以(3)中的d个数必是(4)的全部解．于是$A(d)$中的每个数必有形式a^k，对某个$k=1, 2, \cdots, d$．何时$\exp_p(a^k)=d$？根据引理1，这种情况出现当且仅当$(k, d)=1$时．换言之，在(3)

的d个数中有$\varphi(d)$个数的次数为$d \bmod p$. 这样，我们证明了，当$f(d)\neq 0$时，有$f(d)=\varphi(d)$. 由前面的说明，证明完成.

10.5 原根与二次剩余

定理10.5 令g是模p的一个原根，p是一个奇素数. 则偶次幂

$$g^2,\ g^4,\ \cdots,\ g^{p-1}$$

是模p的二次剩余，而奇次幂

$$g,\ g^3,\ \cdots,\ g^{p-2}$$

是模p的二次非剩余.

证明 如果n是偶数，写$n=2m$，则$g^n=(g^m)^2$，所以

$$g^n \equiv x^2 \pmod p,\ 其中x=g^m,$$

于是$g^n Rp$. 但有$\frac{p-1)}{2}$个不同的偶次幂g^2，…，g^{p-1} modp，这与模p的二次剩余的个数相同，所以偶次幂是二次剩余而奇次幂是二次非剩余.

10.6 模p^α的原根存在

下面我们回到$m=p^\alpha$的情形，其中p是一个奇素数，$\alpha\geq 2$. 在寻找模p^α的原根时，很自然地考虑从模p的原根中挑选. 令g是模p的一个原根并问，是否g也是模p^2的一个原根. 由于$g^{p-1}\equiv 1 \pmod p$，$\varphi(p^2)=p(p-1)>p-1$，如果

$g^{p-1}=1\ (\mathrm{mod}\ p^2)$，那么这个g一定不是模$p^2$的原根．因此，关系式

$$g^{p-1}\not\equiv 1\ (\mathrm{mod}\ p^2)$$

成为g是模p^2的原根的必要条件．应当特别注意的是，这个条件对于g是模p^2的原根也是充分的．更一般，对g是模$p^\alpha(\alpha\geqslant 2)$的原根也是充分的．实际上，我们有下面的定理．

定理10.6　令p是一个奇素数，则有

(a) 如果g是模p的一个原根，则对所有$\alpha\geqslant 1$，g也是模p^α的原根当且仅当

(5) $g^{p-1}\not\equiv 1\ (\mathrm{mod}\ p^2)$．

(b) 模p至少有一个原根g满足(5)，于是，当$\alpha\geqslant 2$时，模p^α至少有一个原根．

证明　我们先证明(b)．令g是模p的一个原根，如果$g^{p-1}\not\equiv 1\ (\mathrm{mod}\ p^2)$就不必证了．如果$g^{p-1}\equiv 1\ (\mathrm{mod}\ p^2)$，我们能证明，模p的另一个原根$g_1=g+p$满足条件

$$g_1^{p-1}\not\equiv 1\ (\mathrm{mod}\ p^2)．$$

实际上，我们有

$$\begin{aligned} g_1^{p-1}&=(g+p)^{p-1}=g^{p-1}+(p-1)g^{p-2}p+tp^2\\ &\equiv g^{p-1}+(p^2-p)g^{p-2} \quad (\mathrm{mod}\ p^2)\\ &\equiv 1-pg^{p-2} \quad (\mathrm{mod}\ p^2)． \end{aligned}$$

但我们不能有$pg^{p-2}\equiv 0\ (\mathrm{mod}\ p^2)$，因为这会推出$g^{m-2}\equiv 0\ (\mathrm{mod}\ p)$与g是p的原根矛盾．于是$g_1^{p-1}\not\equiv 1\ (\mathrm{mod}\ p^2)$，所以(b)得到证明

现在我们证明(a)．设g是模p的一个原根，如果这个g也是模$p^\alpha(\alpha\geqslant 1)$的原根，那么，特别地，它也是模$p^2$的原根，如前所述，得出(5)式成立．

反之，设g是模p的一个原根满足(5)．我们证明，g也是模p^{α}($\alpha \geqslant 2$)的一个原根．令t是g的次数$\bmod p^{\alpha}$．我们希望证明$t=\varphi(p^{\alpha})$．因为$g^{t}\equiv 1 \pmod{p^{\alpha}}$，我们也有$g^{t}\equiv 1 \pmod{p}$，所以$\varphi(p)\mid t$，写

(6) $t=q\varphi(p)$，

由于$t\mid\varphi(p^{\alpha})$，所以$q\varphi(p)\mid\varphi(p^{\alpha})$．但$\varphi(p^{\alpha})=p^{\alpha-1}(p-1)$，于是

$$q(p-1)\mid p^{\alpha-1}(p-1).$$

即$q\mid p^{\alpha-1}$．因此，$q=p^{\beta}$其中$\beta\leqslant\alpha-1$．(6)变为

$$t=p^{\beta}(p-1).$$

如果我们能证明$\beta=\alpha-1$，那么$t=\varphi(p^{\alpha})$并且证明完成．

假设恰好相反，$\beta<\alpha-1$，那么$\beta\leqslant\alpha-2$，我们有

$$t=p^{\beta}(p-1)\mid p^{\alpha-2}(p-1)=\varphi(p^{\alpha-1}),$$

这样，因为$\varphi(p^{\alpha-1})$是t的倍数，推出

(7) $g^{\varphi(p^{\alpha-1})}\equiv 1 \pmod{p^{\alpha}}$．

我们用下面的引理证明(7)是一个矛盾，由此完成本定理的证明．

引理2 令g是模p的一个原根，使得

(8) $g^{p-1}\not\equiv 1 \pmod{p^{\alpha}}$，

那么，对每个$\alpha\geqslant 2$，我们有

(9) $g^{\varphi(p^{\alpha-1})}\not\equiv 1 \pmod{p^{\alpha}}$．

证明　我们对α作归纳法．对$\alpha=2$，(9)就是(8)．于是假设(9)对α成立．根据Euler-Fermat定理我们有

$$g^{\varphi(p^{\alpha-1})}\equiv 1 \pmod{p^{\alpha-1}}$$

所以，

$$g^{\varphi(p^{\alpha-1})}=1+kp^{\alpha-1},$$

因为(9)，所以$p\nmid k$. 上式两端自乘p次，得

$$\begin{aligned} g^{\varphi(p^{\alpha})} &= (1+kp^{\alpha-1})^{p} \\ &= 1+kp^{\alpha}+k^{2}\frac{p(p-1)}{2}p^{2(\alpha-1)} \\ &\quad +rp^{3(\alpha-1)}, \end{aligned}$$

因为$\alpha\geqslant 2$，所以$2\alpha-1\geqslant\alpha-1$，$3\alpha-3\geqslant\alpha+1$，于是上式给出一个同余式

$$g^{\varphi(p^{\alpha})}\equiv 1+kp^{\alpha}\pmod{p^{\alpha+1}},$$

其中$p\nmid k$. 即$g^{\varphi(p^{\alpha})}\not\equiv 1\pmod{p^{\alpha+1}}$，所以，如果(9)对$\alpha$成立，则(9)对$\alpha+1$也成立. 这完成了引理2的证明并且也完成了定理10.6的证明. □

10.7 模$2p^{\alpha}$的原根存在

定理10.7 如果p是一个奇素数并且$\alpha\geqslant 1$，那么存在模p^{α}的一个奇数原根g. 每一个这样的g也是模$2p^{\alpha}$的原根.

证明 如果g是模p^{α}的一个原根，那么$g+p^{\alpha}$也是模p^{α}的一个原根，但g或$g+p^{\alpha}$之一必为奇数，所以模p^{α}的奇数原根总是存在的.

令g是模p^{α}的一个奇数原根，并令f是g的次数$\bmod 2p^{\alpha}$. 我们想证明$f=\varphi(2p^{\alpha})$. 由于$f\mid\varphi(2p^{\alpha})$，$\varphi(2p^{\alpha})=\varphi(2)\varphi(p^{\alpha})=\varphi(p^{\alpha})$，所以$f\mid\varphi(p^{\alpha})$. 另一方面，$g^{f}\equiv 1\pmod{2p^{\alpha}}$，所以$g^{f}\equiv 1\pmod{p^{\alpha}}$. 因为g是模$p^{\alpha}$的一个原根，所以$\varphi(p^{\alpha})\mid f$，因此$f=\varphi(p^{\alpha})=\varphi(2p^{\alpha})$，所以g是模$2p^{\alpha}$的一个原根. □

10.8 其他情况下原根不存在

定理10.8 给定$m\geqslant 1$，m的形式不是$m=1, 2, 4, p^{\alpha}$或$2p^{\alpha}$，其中p是奇素数．则对任何一个与m互素的a，我们有

$$a^{\frac{\varphi(m)}{2}}\equiv 1 \pmod{m},$$

所以模m没有原根．

证明 我们已经证明了，当$\alpha\geqslant 3$时，模2^{α}没有原根．因此，我们假设m有因子分解式

$$m=2^{\alpha}p_1^{\alpha_1}\cdots p_s^{\alpha_s},$$

其中p_i是奇素数$s\geqslant 1$，$\alpha\geqslant 0$．因为m的形式不是1，2，4，p^{α}或$2p^{\alpha}$，所以，当$s=1$时，有$\alpha\geqslant 2$；当$\alpha=0$或1时，有$s\geqslant 2$．注意

$$\varphi(m)=\varphi(2^{\alpha})\varphi(p_1^{\alpha_1})\cdots\varphi(p_s^{\alpha_s}).$$

现在令a是与m互素的任一整数，我们希望证明

$$a^{\frac{\varphi(m)}{2}}\equiv 1 \pmod{m}.$$

令g是模$p_1^{\alpha_1}$的一个原根，选取k，使

$$a\equiv g^{k} \pmod{p_1^{\alpha_1}},$$

则有

$$(10)\quad a^{\frac{\varphi(m)}{2}}\equiv g^{\frac{k\varphi(m)}{2}}\equiv g^{t\varphi(p_1^{\alpha_1})} \pmod{p_1^{\alpha_1}},$$

其中$t=k\varphi(2^{\alpha})\varphi(p_2^{\alpha_2})\cdots\dfrac{\varphi(p_s^{\alpha_s})}{2}$.

我们将证明，t是一个整数．如果$\alpha\geqslant 2$，则因子$\varphi(2^{\alpha})$是偶数，于是t是整数．如果$\alpha=0$或1，则$s\geqslant 2$，因子$\varphi(p_2^{\alpha_2})$是

偶数，所以t仍是整数．于是，同余式(10)给我们

$$a^{\frac{\varphi(m)}{2}} \equiv 1 \pmod{p_1^{\alpha_1}}.$$

用同样方法，我们得

$$(11)\quad a^{\frac{\varphi(m)}{2}} \equiv 1 \pmod{p_i^{\alpha_i}}$$

对每一个$i=1, 2, \cdots, s$．现在我们证明这个同余式对模2^α也成立．如果$\alpha\geqslant 3$，条件$(a, m)=1$要求a是奇数，并且我们可以应用定理10.3写

$$a^{\frac{\varphi(2^\alpha)}{2}} \equiv 1 \pmod{2^\alpha}.$$

因为$\varphi(2^\alpha)|\varphi(m)$，这给我们

$$(12)\quad a^{\frac{\varphi(m)}{2}} \equiv 1 \pmod{2^\alpha} \quad \alpha\geqslant 3.$$

如果$\alpha\leqslant 2$，我们有

$$(13)\quad a^{\varphi(2^\alpha)} \equiv 1 \pmod{2^\alpha}.$$

但$s\geqslant 1$，所以$\varphi(m)=\varphi(2^\alpha)\varphi(p_1^{\alpha_1})\cdots\varphi(p_s^{\alpha_s})=2r\varphi(2^\alpha)$，其中r是整数．于是$\varphi(2^\alpha)\Big|\dfrac{\varphi(m)}{2}$，由(13)推出(12)对$\alpha\leqslant 2$也成立，于是(12)对所有的$\alpha$成立．(11)与(12)的模乘在一起，我们得

$$a^{\frac{\varphi(m)}{2}} \equiv 1 \pmod{m}.$$

这证明a不能是模m的原根．□

10.9 模m的原根的个数

我们已经证明，一个$\geqslant 1$的整数m有原根当且仅当

$m=1, 2, 4, p^\alpha$或$2p^\alpha$，

其中p是一个奇素数并且$\alpha\geqslant1$．下面的定理告诉我们，对每个这样的m，有多少个原根存在．定理10.9 如果m有一个原根g，那么m恰有$\varphi(\varphi(m))$个不同余的原根，并且这些原

表10.1 素数p的最小原根g(p)

p	g(p)	p	g(p)	p	g(p)	p	g(p)	p	g(p)	p	g(p)
2	1	109	6	269	2	439	15	617	3	811	3
3	2	113	3	271	6	443	2	619	2	821	2
5	2	127	3	277	5	449	3	631	3	823	3
7	3	131	2	281	3	457	13	641	3	827	2
11	2	137	3	283	3	461	2	643	11	829	2
13	2	139	2	293	2	463	3	647	5	839	11
17	3	149	2	307	5	467	2	653	2	853	2
19	2	151	6	311	17	479	13	659	2	857	3
23	5	157	5	313	10	487	3	661	2	859	2
29	2	163	2	317	2	491	2	673	5	863	5
31	3	167	5	331	3	499	7	677	2	877	2
37	2	173	2	337	10	503	5	683	5	881	3
41	6	179	2	347	2	509	2	691	3	883	2
43	3	181	2	349	2	521	3	701	2	887	5
47	5	191	19	353	3	523	2	709	2	907	2
53	2	193	5	359	7	541	2	719	11	911	17
59	2	197	2	367	6	547	2	727	5	919	7
61	2	199	3	373	2	557	2	733	6	929	3
67	2	211	2	379	2	563	2	739	3	937	5
71	7	223	3	383	5	569	3	743	5	941	2
73	5	227	2	389	2	571	3	751	3	947	2
79	3	229	6	397	5	577	5	757	2	953	3
83	2	233	3	401	3	587	2	761	6	967	5
89	3	239	7	409	21	593	3	769	11	971	6
97	5	241	7	419	2	599	7	773	2	977	3
101	2	251	6	421	2	601	7	787	2	983	3
103	5	257	3	431	7	607	3	797	2	997	7
107	2	263	5	433	5	613	2	809	3		

根由集合

$$S=\{g^n:1\leqslant n\leqslant\varphi(m),\ (n,\ \varphi(m))=1\}$$

中的数给出.

证明　我们有$\exp_m(g)=\varphi(m)$. 由引理1，当且仅当$(n,\ \varphi(m))=1$时，$\exp_m(g^n)=\exp_m(g)$，因此集合S中的每一个元素都是模m的原根.

反之，如果a是模m的一个原根，则对某个$k=1,\ 2,\ \cdots,\ \varphi(m)$，有$a\equiv g^k\ (\mathrm{mod}\,m)$，于是$\exp_m(g^K)=\exp_m(a)=\varphi(m)$，由引理1，$(K,\ \varphi(m))=1$，因此任一原根都是S中的一个数. 因此S包含有$\varphi[\varphi(m)]$个互不同余的数modm，所以证明完成. □

虽然我们证明了某些模的原根的存在性，但若不用大量的计算，一般还不知道求这些原根的直接的方法，特别是对很大的模. 令$g(p)$表示模p的最小原根，表10.1列出所有$\leqslant1000$的奇素数p的$\varphi(p)$.

10.10　指数的计算

如果m有一个原根g，那么$1,\ g,\ g^2,\ \cdots,\ g^{\varphi(m)-1}$形成模m的一个简化剩余系. 如果$(a,\ m)=1$，那么在区间$0\leqslant k\leqslant\varphi(m)-1$里有唯一的一个整数k，使得

$$a\equiv g^k\quad(\mathrm{mod}\,m),$$

这个整数k叫做以g为底，a对模m的指数，并写为

$$k=\mathrm{ind}_g a,$$

或略去底数g，简记为$k=\mathrm{ind}\,a$.

下面的定理表明，指数有许多类似于对数的性质，其证

明作为练习留给读者.

定理10.10 令g是模m的一个原根. 如果$(a,m)=(b,m)=1$, 则有

(a) $\text{ind}ab \equiv \text{ind}a+\text{ind}b \pmod{\varphi(m)}$;

(b) $\text{ind}a^n \equiv n\,\text{ind}a \pmod{\varphi(m)}$, $n \geqslant 1$;

(c) $\text{ind}1=0$, $\text{ind}g=1$;

(d) $\text{ind}(-1)=\frac{\varphi(m)}{2}$, 若$m \geqslant 2$;

(e) 如果g′也是模m的一个原根, 则

$$\text{ind}_g a \equiv \text{ind}_{g'} a \cdot \text{ind}_g g' \pmod{\varphi(m)}. \quad \square$$

下面几个例子说明指数在解同余式中的应用.

例1 一次同余式、假设m有一个原根, 并令$(a, m)=(b, m)=1$, 则一次同余式

(14) $ax \equiv b \pmod{m}$

等价于同余式

$$\text{ind}a+\text{ind}x \equiv \text{ind}b \pmod{\varphi(m)},$$

所以(14)的唯一解满足同余式

$$\text{ind}x \equiv \text{ind}b-\text{ind}a \pmod{\varphi(m)}.$$

作为一个数值的例子, 我们考虑一次同余式

$$9x \equiv 13 \pmod{47},$$

对应的指数式是

$$\text{ind}x \equiv \text{ind}13-\text{ind}9 \pmod{46}.$$

由表10.2我们得$\text{ind}13=11$, $\text{ind}9=40$ (对$p=47$), 所以

$$\text{ind}x \equiv 11-40 \equiv -29 \equiv 17 \pmod{46},$$

再由表10.2, 我们得$x \equiv 38 \pmod{47}$.

例2　二项式同余式．形如

$$x^n \equiv a \pmod{m}$$

的同余式称为二项式同余式．如果m有原根并且$(a, m)=1$，则此同余式等价于同余式

$$n\,\mathrm{ind}x \equiv \mathrm{ind}a \pmod{\varphi(m)}.$$

这是一个以indx为未知量的一次同余式．于是，当且仅当a被$d=(n, \varphi(m))$整除时，这个同余有解．在有解的情况下，它恰有d个解．

用一个数字的例子来说明．考虑二项式同余式

(15) $x^8 \equiv a \pmod{17}$，

对应的指数式是

(16) $8\,\mathrm{ind}x \equiv \mathrm{ind}a \pmod{16}$.

这里$d=(8, 16)=8$．由于1与16是指数被8整除的仅有的两个数mod17．实际上，$\mathrm{ind}1=0$，$\mathrm{ind}16=8$，所以(15)在$a \not\equiv 1$或$a \not\equiv 16 \pmod{17}$时没有解．

对于$a=1$，同余式(16)变为

(17) $8\,\mathrm{ind}x \equiv 0 \pmod{16}$

而对于$a=16$，它变为

(18) $8\,\mathrm{ind}x \equiv 8 \pmod{16}$.

(17)与(18)中的每一个都恰有8个解mod16．(17)的解是指数为偶数的x，

$$x \equiv 1, 2, 4, 8, 9, 13, 15, 16 \pmod{17}.$$

当然，这些都是17的二次剩余．(18)的解是指数为奇数的x，也就是17的二次非剩余，

$$x \equiv 3, 5, 6, 7, 10, 11, 12, 14 \pmod{17}.$$

例3　指数同余式．形如

表10.2 对奇素数p<50，所有的数a≢0(modp)的指数。其中底数g是p的最小原根

a	素数 3	5	7	11	13	17	19	23	29	31	37	41	43	47
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	1	1	2	1	1	14	1	2	1	24	1	26	27	18
3		3	1	8	4	1	13	16	5	1	26	15	1	20
4		2	4	2	2	12	2	4	2	18	2	12	12	36
5			5	4	9	5	16	1	22	20	23	22	25	1
6			3	9	5	15	14	18	6	25	27	1	28	38
7				7	11	11	6	19	12	28	32	39	35	32
8				3	3	10	3	6	3	12	3	38	39	8
9				6	8	2	8	10	10	2	16	30	2	40
10				5	10	3	17	3	23	14	24	8	10	19
11					7	7	12	9	25	23	30	3	30	7
12					6	13	15	20	7	19	28	27	13	10
13						4	5	14	18	11	11	31	32	11
14						9	7	21	13	22	33	25	20	4
15						6	11	17	27	21	13	37	26	21
16						8	4	8	4	6	4	24	24	26
17							10	7	21	7	7	33	38	16
18							9	12	11	26	17	16	29	12
19								15	9	4	35	9	19	45
20								5	24	8	25	34	37	37
21								13	17	29	22	14	36	6
22								11	26	17	31	29	15	25
23									20	27	15	36	16	5
24									8	13	29	13	40	28
25									16	10	10	4	8	2
26									19	5	12	17	17	29
27									15	3	6	5	3	14
28									14	16	34	11	5	22
29										9	21	7	41	35
30										15	14	23	11	39

a	素数													
	3	5	7	11	13	17	19	23	29	31	37	41	43	47
31											9	28	34	3
32											5	10	9	44
33											20	18	31	27
34											8	19	23	34
35											19	21	18	33
36											18	2	14	30
37												32	7	42
38												35	4	17
39												6	33	31
40												20	22	9
41													6	15
42													21	24
43														13
44														43
45														41
46														23

$$a^x \equiv b \quad (\bmod m)$$

的同余式是一个指数同余式．如果m有原根，并且$(a, m)=(b, m)=1$，则此同余式等价于一次同余式

(19) $x\,\mathrm{ind}a \equiv \mathrm{ind}b \quad (\bmod \varphi(m))$.

令$d=(\mathrm{ind}a, \varphi(m))$，那么(19)有解当且仅当$d|\mathrm{ind}b$．在有解时，恰有d个解．例如，

(20) $25^x \equiv 17 \quad (\bmod 47)$.

我们有$\mathrm{ind}25=2$，$\mathrm{ind}17=16$，$d=(2, 46)=2$，因(19)变为

$$2x \equiv 16 \quad (\bmod 46),$$

它有两个解$x \equiv 8$与$31\ (\bmod 46)$，这也是(20)的解mod47.

10.11 原根与Dirichlet特征

显然能利用原根与指数去构造模m的所有的Dirichlet特征．首先我们考虑一个素数幂的模p^α，这里p是一个奇素数并且$\alpha\geqslant 1$．

令g是模p的一个原根，并且g也是模p^β的一个原根对所有$\beta\geqslant 1$．根据定理10.6，这样的一个g是存在的．如果$(n,p)=1$，则令$b(n)\equiv \mathrm{ind}_g n \pmod{p^\alpha}$，那么$b(n)$是唯一的满足下式的整数，

$$n\equiv g^{b(n)} \pmod{p^\alpha} \quad 0\leqslant b(n)<\varphi(p^\alpha).$$

对于$h=0, 1, 2, \cdots, \varphi(p^\alpha)-1$，由

$$(21)\quad \chi_h(n)=\begin{cases} e^{\frac{2\pi i h b(n)}{\varphi(p^\alpha)}} & 若p\nmid n \\ 0 & 若p\mid n \end{cases}$$

定义χ_h．利用指数的性质，容易验证χ_h是完全积性的，并且是一个以p^α为周期的周期函数，所以χ_h是模p^α的一个Dirichlet特征．其证明作为习题留给读者．

因为

$$\chi_h(g)=e^{\frac{2\pi i h}{\varphi(p^\alpha)}},$$

所以特征$\chi_0, \chi_1, \cdots, \chi_{\varphi(p^\alpha)-1}$是互不相同的，这因为它们在g上取不同的值．故有$\varphi(p^\alpha)$个这样的函数表示了模$p^\alpha$的所有的Dirichlet特征．以$g=3$为原根，同样可以构造模$2^\alpha$（$\alpha=1$或$\alpha=2$）的所有的Dirichlet特征．

如果$m=p_1^{\alpha_1}\cdots p_r^{\alpha_r}$，其中$p_i$是不同的奇素数，并且$\chi_i$是模$p_i^{\alpha_i}$的一个Dirichlet特征，那么乘积$\chi=\chi_1\cdots\chi_r$就是模

m的一个Dirichlet特征．因为$\varphi(m)=\varphi(p_1^{\alpha_1})\cdots\varphi(p_i^{\alpha_i})$，所以，当每个$x_i$通过模$p_i^{\alpha_i}$的$\varphi(p_i^{\alpha_i})$个特征时，我们就得到$\varphi(m)$个这样的特征．于是，对每一个奇数模，我们显然能构造模m的所有特征．

如果$\alpha\geqslant3$，则模2^α没有原根．为了得到模2^α的特征，构造的方法有必要作些微小的变化．下面的定理证明，5是模2^α的原根的一个很好的替代者．

定理10.11　设$\alpha\geqslant3$，那么对每一个奇数n，有唯一确定的整数b(n)，使得

$$n\equiv(-1)^{\frac{(n-1)}{2}}5^{b(n)}\quad(\bmod 2^\alpha),$$

$$1\leqslant b(n)\leqslant\frac{\varphi(2^\alpha)}{2}.$$

证明　令$f=\exp_{2^\alpha}(5)$，于是$5^f\equiv1\ (\bmod 2^\alpha)$．我们将证明$f=\frac{\varphi(2^\alpha)}{2}$．因为$f\mid\varphi(2^\alpha)=2^{\alpha-1}$，所以有$f=2^\beta$对某个$\beta\leqslant\alpha-1$．由定理10.8我们知道，

$$5^{\frac{\varphi(2^\alpha)}{2}}\equiv1\quad(\bmod 2^\alpha),$$

于是$f\leqslant\frac{\varphi(2^\alpha)}{2}$，因此$\beta\leqslant2$．下面我们证明$\beta=\alpha-2$．

等式$5=1+2^2$两边自乘$f=2^\beta$次，得

$$5^f=(1+2^2)^{2^\beta}=1+2^{\beta+2}+r2^{\beta+3}$$
$$=1+2^{\beta+2}(1+2r),$$

其中r是一个整数．于是$5^f-1=2^{\beta+2}t$，其中t是一个奇数．但$2^\alpha\mid5^f-1$，所以$\alpha\leqslant\beta+2$或$\beta\geqslant\alpha-2$，于是$\beta=\alpha-2$并且$f=2^{\alpha-2}=\frac{\varphi(2^\alpha)}{2}$．因此，

(22) $5, 5^2, \cdots, 5^f$

对模2^α互不同余，而每一个对模4都同余于1，这是因为$5\equiv 1\pmod 4$．类似地，

(23) $-5, -5^2, \cdots, -5^f$

对模2^α也互不同余，而每一个对模4都同余于3，这因为$-5\equiv 3\pmod 4$．在(22)与(23)里共有$2f=\varphi(2^\alpha)$个数，而且也不能有$5^a\equiv -5^b\pmod{2^\alpha}$，因为这将得出$1\equiv -1\pmod 4$．于是(22)与(23)里的数表示了$\varphi(2^\alpha)$个不同余的奇数$\bmod 2^\alpha$．每一个对模4同余于1的奇数n必与(22)里一个数同余$\bmod 2^\alpha$，每一个对模4同余于3的奇数必与(23)里的一个数同余$\bmod 2^\alpha$．定理得证． □

借助于定理10.11我们能构造模$2^\alpha(\alpha\geqslant 3)$的所有的特征．令

$$(24)\quad f(n)=\begin{cases}(-1)^{\frac{(n-1)}{2}} & n\text{为奇数，}\\ 0 & n\text{为偶数，}\end{cases}$$

并令

$$g(n)=\begin{cases}e^{\frac{2\pi i b(n)}{2^{\alpha-2}}} & n\text{为奇数，}\\ 0 & n\text{为偶数，}\end{cases}$$

其中$b(n)$是根据定理10.11给定的整数．容易验证，f与g都是模2^α的特征，乘积

(25) $x_{a,c}(n)=f(n)^a g(n)^c$

也是模2^α的特征，其中$a=1,2$而$c=1,2,\cdots,\varphi\frac{(2^\alpha)}{2}$，并且这$\varphi(2^\alpha)$个特征是不同的，所以它们表示了模$2^\alpha$的所有特征．

如果$m=2^{\alpha}Q$，这里Q是奇数，我们作乘积$x=x_1x_2$，其中x_1通过模2^{α}的$\varphi(2^{\alpha})$个特征，x_2通过模Q的$\varphi(Q)$个特征，这样，就得到模m的所有的特征．

10.12 模p^{α}的实值Dirichlet特征

如果x是模m的一个实值Dirichlet特征，并且$(n, m)=1$，那么数$x(n)$是一对实的单位根，所以$x(n)=\pm 1$．由上一节的构造我们能确定模P^{α}的所有的实值Dirichlet特征．

定理10.12　对每一个奇素数p与$\alpha\geqslant 1$，考虑由(21)给出的模P^{α}的$\varphi(p^{\alpha})$个Dirichlet特征．那么，当且仅当$h=0$或$h=\frac{\varphi(p^{\alpha})}{2}$时，$x_h$是实的．于是模$P^{\alpha}$恰有两个实特征．

证明　我们有，$e^{2\pi iz}=1$当且仅当z是整数．如果$P\nmid n$，则有

$$x_h(n)=e^{\frac{2\pi ihb(n)}{\varphi(p^{\alpha})}}$$

所以$x_h(n)=\pm 1$当且仅当$\varphi(p^{\alpha})\mid 2hb(n)$．如果$h=0$或$h=\frac{\varphi(p^{\alpha})}{2}$，这个条件对所有的n是满足的．反之，如果对所有的n，有$\varphi(p^{\alpha})\mid 2hb(n)$，则当$b(n)=1$时，我们有$\varphi(p^{2})\mid 2h$或$\frac{\varphi(p^{\alpha})}{2}\Big| h$，于是$h=0$或$h=\frac{\varphi(p^{\alpha})}{2}$，因为它们是小于$\varphi(p^{\alpha})$的仅有的$\frac{\varphi(p^{\alpha})}{2}$的倍数．

注意：对应于$h=0$的特征是主特征．当$\alpha=1$时，二次特征$x(n)=\left(\frac{n}{p}\right)$是模p的另一个唯一的实值特征．

对于m＝1，2与4，所有的Dirichlet特征都是实的．下面的定理描述了模$2^\alpha(\alpha\geqslant 3)$的实值特征．

定理10.13　如果$\alpha\geqslant 3$，考虑由(25)给出的模2^α的$\varphi(2^\alpha)$个Dirichlet特征$\chi_{a,c}$．则$\chi_{a,c}$是实值的当且仅当$c=\frac{\varphi(2^\alpha)}{2}$或$c=\frac{\varphi(2^\alpha)}{4}$．于是模$2^\alpha(\alpha\geqslant 3)$恰有4个实特征．

证明　如果$\alpha\geqslant 3$并且n是奇数，根据(25)，有

$$\chi_{a,c}(n)=f(n)^a g(n)^c,$$

其中$f(n)=\pm 1$而

$$g(n)^c=e^{\frac{2\pi i c b(n)}{2^{\alpha-2}}},$$

其中$1\leqslant c\leqslant 2^{\alpha-2}$。当且仅当$2^{\alpha-2}\mid 2cb(n)$或$2^{\alpha-3}\mid cb(n)$时，$g(n)^c=\pm 1$．因为$\varphi(2^\alpha)=2^{\alpha-1}$，所以当$c=\frac{\varphi(2^\alpha)}{2}=2^{\alpha-2}$或$c=\frac{\varphi(2^\alpha)}{4}=2^{\alpha-3}$时，上面的条件是满足的．反之，如果对所有的n，有$2^{\alpha-3}\mid cb(n)$，那么由$b(n)=1$要求$2^{\alpha-3}\mid c$，所以$c=2^{\alpha-3}$或$2^{\alpha-2}$，这是因为$1\leqslant c\leqslant 2^{\alpha-2}$．　□

10.13　模p^α的本原Dirichlet特征

在定理8.14时，我们证明了，当p是奇素数时，模p的每一个非主特征χ都是本原的，现在，我们来确定模p^2的所有的本原特征．

我们回忆8.7节里讲过的，χ是模k的本原特征当且仅当χ没有诱导模d＜k．一个诱导模d是k的一个约数，它满足

$$\chi(n)=1 \quad 当(n,k)=1,\ n\equiv 1(\bmod d)时.$$

如果$k=p^{\alpha}$并且χ是模p^{α}的非本原特征，那么约数 1，p，…，$p^{\alpha-1}$之一是诱导模，于是$p^{\alpha-1}$是一个诱导模．因此，当且仅当$n^{\alpha-1}$不是χ的一个诱导模时，χ是p^{α}的本原特征．

定理10.14 **对一个奇素数p与$\alpha\geqslant 2$，考虑由(21)给出的模p^{α}的$\varphi(p^{\alpha})$个Dirichlet特征χ_h，则χ_h是模p^{α}的本原特征当且仅当$p\nmid h$．**

证明　我们证明$p^{\alpha-1}$是一个诱导模当且仅当$p|h$．如果$p\nmid h$，根据(21)式，我们有

$$\chi_h(n)=e^{\frac{2\pi i h b(n)}{\varphi(p^{\alpha})}},$$

其中$n\equiv g^{b(n)}(\bmod p^{\alpha})$．对所有$\beta\geqslant 1$，$g$是模$p^{\beta}$的原根．因此$g^{b(n)}\equiv n(\bmod p^{\alpha-1})$．如果$n\equiv 1(\bmod p^{\alpha-1})$，则$g^{b(n)}\equiv 1(\bmod p^{\alpha-1})$，并因为$g$是$p^{\alpha-1}$的一个原根，所以有$\varphi(p^{\alpha-1})|b(n)$或

$$b(n)=t\varphi(p^{\alpha-1})=\frac{t\varphi(p^{\alpha})}{p}$$

对某个整数t.因此

$$\chi_h(n)=e^{\frac{2\pi i h t}{p}}.$$

如果$p\nmid h$，则$\chi_h(n)=1$，于是χ_h是模p^{α}的非本原特征．如果$p\nmid h$，取$n=1+p^{\alpha-1}$，则$n\equiv 1(\bmod p^{\alpha-1})$，但$n\not\equiv 1(\bmod p^{\alpha})$，所以$0<b(n)<\varphi(p^{\alpha})$．因此$p\nmid t$，$p\nmid ht$并且$\chi_h(n)\neq 1$．这证明了，当$p\nmid h$时，$\chi_h$是本原的．　□

当$m=1$或2时，模m仅有一个特征χ，即主特征．如果$m=4$，则模4有两个特征，就是主特征与由(24)给出的本

原特征．下面的定理描述模$2^{\alpha}(\alpha\geqslant3)$的所有的本原特征．其证明与定理10.14的证明类似并留给读者．

定理10.15 **如果$\alpha\geqslant3$，考虑由(25)式给出的模2^{α}的$\varphi(2^{\alpha})$个Dirichlet特征$\chi_{a,c}$．则$\chi_{a,c}$是模2^{α}的本原特征当且仅当c是奇数．**

前面的结果描述了所有素数幂p^{α}为模的所有本原特征．为了确定一个复合数模k的本原特征，我们写

$$k=p_1^{\alpha_1}\cdots p_r^{\alpha_r}.$$

于是模k的每一特征χ有因子分解形式

$$\chi=\chi_1\cdots\chi_r,$$

其中每个χ_i是模$p_i^{\alpha_i}$的一个特征．另外，根据习题8.12，χ是模k的本原特征当且仅当每一个χ_i是模$p_i^{\alpha_i}$的本原特征．因此，我们完全描述了模k的所有本原特征．

第十章习题

1. 证明，m是素数当且仅当$\exp_m(a)=m-1$对某个a成立．
2. 如果$(a,m)=(b,m)=1$，且$(\exp_m(a),\exp_m(b))=1$，

证明

$$\exp_m(ab)=\exp_m(a)\exp_m(b).$$

3. 令g是素数p的一个原根，证明，如果$p\equiv1(\mathrm{mod}\ 4)$，则$-g$也是p的一个原根；如果$p\equiv3(\mathrm{mod}\ 4)$，则$\exp_p(-g)=\frac{(p-1)}{2}$.

4. (a) 如果p是一个形如$2^n+1(n>1)$的素数，证明3是p的一个原根.

(b) 如果p是一个形如$4q+1$的素数，其中q是一个奇素数. 证明2是模p的一个原根.

5. 令$m>2$是一个有原根的整数且$(a,m)=1$，如果存在一个x，使得$a\equiv x^2(\bmod m)$，我们就记为aRm. 证明

(a) aRm当且仅当$a^{\frac{\varphi(m)}{2}}\equiv 1(\bmod\ m)$，

(b) 如果aRm，则同余式$x^2\equiv a(\bmod m)$恰有两个解.

(c) 有且仅有$\frac{\varphi(m)}{2}$个互不同余modm的整数a，使得$(a,m)=1$并且aRm.

6. 设$m>2$，$(a,m)=1$，aRm. 证明，同余式$x^2\equiv a(\bmod\ m)$恰有两个解当且仅当m有原根.

7. 令$S_n(p)=\sum_{k=1}^{p-1}k^n$，其中p是一个奇素数且$n>1$，证明

$$S_n(p)\equiv\begin{cases}0 \quad (\bmod\ p) & 若 n\not\equiv 0(\bmod\ p-1).\\ 1 \quad (\bmod\ p) & 若 n\equiv 0(\bmod\ p-1).\end{cases}$$

8. 证明，模p的全部原根之和同余于$\mu(p-1)\bmod p$.

9. 如果p是一个>3的奇素数，证明，模p的全部原根之积同余于1modp.

10. 令p是一个形如$2^{a^k}+1$的奇素数. 证明，模p的全部原根的集合等于模p的全部二次非剩余的集合. 利用此结果证明，7是任意这样的素数的一个原根.

11. 设$d|\varphi(m)$，如果$d=\exp_m(a)$，我们就说a是同余式

$x^d \equiv 1 \pmod m$

的一个原根．证明，如果同余式

$x^{\varphi(m)} \equiv 1 \pmod m$

有一个原根，那么，它就有$\varphi(\varphi(m))$个对模m互不同余的原根．

12．证明定理10.10里叙述的指数的性质．

13．令p是一个奇素数．如果$(h,p)=1$，则令

$S(h)=\{h^n: 1 \leqslant n \leqslant \varphi(p-1),\ (n,p-1)=1\}$.

如果h是p的一个原根，那么集合S(h)中各数对模p互不同余．（实际上，它们是p的原根．）证明，当且仅当$p \equiv 3 \pmod 4$时，存在一个整数h，它不是p的原根，使S(h)中各数对模p互不同余．

14．如果$m>1$，令$p_1, \cdots, p_k$是$\varphi(m)$的不同的素因子．如果$(g, m)=1$，证明，g是m的一个原根当且仅当

$g^{\frac{\varphi(m)}{p_i}} \not\equiv 1 \pmod m$, $i=1, 2, \cdots, k$.

15．素数$p=71$有一个原根7．找出71的所有的原根，并找出p^2与$2p^a$的一个原根．

16．解下列同余式：

(a) $8x \equiv 7 \pmod{43}$,

(b) $x^8 \equiv 17 \pmod{43}$,

(c) $8^x \equiv 3 \pmod{43}$

17．令q是一个奇素数并设$p=4q+1$也是素数．

(a) 证明同余式$x^2 \equiv -1 \pmod p$有且仅有两个解，每个解都是p的二次非剩余．

(b) 证明，除开(a)里的两个二次非剩余之外，p的任

一个二次非剩余都是p的原根.

(c) 找出29的全部原根.

18. 17题的推广. 令q是一个奇素数并设$p=2^nq+1$也是素数. 证明, 如果$a^{2^n}\not\equiv 1 \pmod{p}$, 则p的任一二次非剩余a都是p的原根.

19. 证明, 模8只有两个实本原特征, 并作出一个表显示它们的值.

20. 令x是模m的一个实本原特征. 如果m不是2的方幂, 证明m有形式

$$m=2^{\alpha}p_1\cdots p_r,$$

其中p_i是不同的奇素数并且$\alpha=0$, 2或3. 如果$\alpha=0$, 证明

$$x(-1)=\prod_{p\mid m}(-1)^{\frac{(p-1)}{2}}.$$

当$\alpha=2$时, 找出$x(-1)$的一个相应的公式.

第十一章　Dirichlet级数与Euler乘积

11.1　引言

1737年，Euler用证明对所有素数展开的级数 $\sum p^{-1}$ 发散的方法证明了无穷多个素数存在性的Euclid定理．他推出这个结论是由下述事实得来的：由

$$(1)\quad \zeta(s)=\sum_{n=1}^{\infty}\frac{1}{n^s}\qquad 对实数s>1$$

给定的zeta函数$\zeta(s)\to\infty$（当$s\to 1$时）．1837年，由于研究级数

$$(2)\quad L(s,x)=\sum_{n=1}^{\infty}\frac{x(n)}{n^s},$$

其中x是一个Dirichlet特征并且$s>1$，Dirichlet证明了他的关于算术级数里素数的著名定理．级数(1)与(2)是形如

$$(3)\quad \sum_{n=1}^{\infty}\frac{f(n)}{n^s}$$

的级数的例子，其中f(n)是一个数论函数．这类级数叫做具有系数f(n)的Dirichlet级数，它们成为解析数论里很有用的工具之一．

本章研究Dirichlet级数的一般性质．下一章作Riemann

zeta函数$\zeta(s)$与Dirichlet L—函数$L(s,\chi)$的更详细的研究.

Riemann记号. 我们令s是一个复变量并写

$$s=\sigma+it,$$

其中σ与t是实数. 则有$n^s=e^{s\log n}=e^{(\sigma+it)\log n}=n^\sigma e^{it\log n}$，这证明$|n^s|=n^\sigma$，因为对实数Q，$|e^{iQ}|=1$.

满足$\sigma>a$的点$s=\sigma+it$的集合叫做是一个半平面，我们将证明，对每一个Dirichlet级数，有一个半平面$\sigma>\sigma_c$，级数在其中收敛，而在另一个半平面$\sigma>\sigma_a$里，级数绝对收敛. 我们还将证明，在收敛半平面里，此级数表示复变量s的一个解析函数.

11.2 Dirichlet级数绝对收敛的半平面

首先，我们注意到，如果$\sigma\geqslant a$，我们有$|n^s|=n^\sigma\geqslant n^a$，于是

$$\left|\frac{f(n)}{n^s}\right|\leqslant\frac{|f(n)|}{n^a}$$

因此，如果Dirichlet级数$\sum f(n)n^{-s}$对于$s=a+ib$绝对收敛，那么根据比较检验法，它对所有的$s(\sigma\geqslant a)$也绝对收敛，由此推出下面的定理.

定理11.1 设级数$\sum|f(n)n^{-s}|$不是对所有s都收敛，也不是对所有s都发散，那么存在一个实数σ_a，叫做绝对收敛的横坐标，使得，当$\sigma>\sigma_a$时，级数$\sum f(n)n^{-s}$绝对收敛，但若$\sigma<\sigma_a$，级数就不绝对收敛.

证明　令D是使$\sum|f(n)n^{-s}|$发散的所有实数σ的集合.

由于级数不是对所有s都收敛，所以D是非空的，又因为级数不是对所有s都发散，所以D有上界，因此D有一个上确界，记为σ_a．如果$\sigma<\sigma_a$，则$\sigma\in D$，否则σ将是D的一个小于上确界的上界．如果$\sigma>\sigma_a$，因为σ_a是D的上确界，故$\sigma\notin D$．定理得证． □

注意，如果级数$\sum|f(n)n^{-s}|$处处收敛，我们就规定$\sigma_a=-\infty$．如果级数$\sum|f(n)n^{-s}|$处处不收敛，我们就规定$\sigma_a=+\infty$．

例 1 Riemann zeta函数．Dirichlet级数$\sum_{n=1}^{\infty}n^{-s}$对$\sigma>1$绝对收敛，当$s=1$时，级数发散，所以$\sigma_a=1$．此级数之和记为$\zeta(s)$并称为Riemann zeta函数．

例 2 如果f有界，即$|f(n)|\leqslant M$对所有的$n\geqslant1$，那么$\sum f(n)n^{-s}$对$\sigma>1$绝对收敛，所以$\sigma_a\leqslant1$．特别，如果x是一个Dirichlet特征，那么L—级数$L(s,x)=\sum x(n)n^{-s}$对$\sigma>1$绝对收敛．

例 3 级数$\sum n^n n^{-s}$对每一个s都发散，所以$\sigma_a=+\infty$．

例 4 级数$\sum n^{-n}n^{-s}$对每一个s都绝对收敛，所以$\sigma_a=-\infty$．

11.3 由Dirichlet级数定义的函数

假设$\sum f(n)n^{-s}$对$\sigma>\sigma_a$收敛并令F(s)表示和函数

$$(4)\quad F(s)=\sum_{n=1}^{\infty}\frac{f(n)}{n^s}\qquad 对\sigma>\sigma_a.$$

本节推出F(s)的一些性质，我们先证明下面的引理．

引理 1 **如果$N\geqslant1$并且$\sigma\geqslant c>\sigma_a$，则有**

$$\left|\sum_{n=N}^{\infty} f(n)n^{-s}\right| \leqslant N^{-(\sigma-c)} \sum_{n=N}^{\infty} |f(n)| n^{-c}.$$

证明　我们有

$$\left|\sum_{n=N}^{\infty} f(n)n^{-s}\right| \leqslant \sum_{n=N}^{\infty} |f(n)| n^{-\sigma}$$

$$= \sum_{n=N}^{\infty} |f(n)| n^{-c} n^{-(\sigma-c)} \leqslant N^{-(\sigma-c)}$$

$$\sum_{n=N}^{\infty} |f(n)| n^{-c}.$$ □

下面的定理描述F(s)的情况，当$x \to +\infty$时.

定理11.2　如果F(s)由(4)给定，则

$$\lim_{\sigma \to +\infty} F(\sigma + it) = f(1).$$

对$-\infty < t < +\infty$**是一致收敛的.**

证明　因为$F(s) = f(1) + \sum_{n=2}^{\infty} f(n)n^{-s}$，所以我们只需证明，当$\sigma \to +\infty$时，第二项趋于0即可. 选取$c > \sigma_a$，则对于$\sigma \geqslant c$，由引理得

$$\left|\sum_{n=2}^{\infty} \frac{f(n)}{n^s}\right| \leqslant 2^{-(\sigma-c)} \sum_{n=2}^{\infty} |f(n)| n^{-c} = \frac{A}{2^\sigma},$$

其中A对于σ与t是独立的. 因为$\frac{A}{2^\sigma} \to 0$（当$\sigma \to +\infty$时），于是定理得证. □

例　当$\sigma \to +\infty$时，$\zeta(\sigma + it) \to 1$且$L(\sigma + it, \chi) \to 1$.

下面我们证明，所有的系数被和函数唯一确定.

定理11.3　唯一性定理. 已知两个Dirichlet级数

$$F(s) = \sum_{n=1}^{\infty} \frac{f(n)}{n^s} \text{与} G(s) = \sum_{n=1}^{\infty} \frac{g(n)}{n^s}$$

对$\sigma > \sigma_a$**都是绝对收敛的. 如果对一个无穷序列**$\{s_k\}$**里的每一s，有**$F(s) = G(s)$**，其中**$k \to \infty$**时，**$\sigma_k \to +\infty$**. 那么，对**

每一个n都有$f(n)=g(n)$.

证明　令$h(n)=f(n)-g(n)$并令$H(s)=F(s)-G(s)$. 则对每一个K，$H(s_k)=0$. 为证明对所有的n，有$h(n)=0$，我们设对某些n有$h(n)\neq 0$并得到一个矛盾.

令N是使$h(n)\neq 0$的最小整数，那么

$$H(s)=\sum_{n=N}^{\infty}\frac{h(n)}{n^s}=\frac{h(N)}{N^s}+\sum_{n=N+1}^{\infty}\frac{h(n)}{n^s},$$

于是

$$h(N)=N^sH(s)-N^s\sum_{n=N+1}^{\infty}\frac{h(n)}{n^s}.$$

令$s=s_k$，我们有$H(s_k)=0$，于是

$$h(N)=-N^{s_k}\sum_{n=N+1}^{\infty}h(n)n^{-s_k}.$$

选取K，使$\sigma_k>c$，其中$c>\sigma_a$，于是由引理1得

$$|h(N)|\leqslant N^{\sigma_k}(N+1)^{-(\sigma_k-c)}\sum_{n=N+1}^{\infty}|h(n)|n^{-c}$$

$$=\left(\frac{N}{N+1}\right)^{\sigma_k}A,$$

其中A对于K是独立的. 令$K\to\infty$，我们得$\left(\frac{N}{N+1}\right)^{\sigma_k}\to 0$，所以$h(N)=0$，这是一个矛盾. □

唯一性定理推出Dirichlet级数不为零的半平面的存在性.（当然，除非此级数恒为0.）

定理11.14　令$F(s)=\sum f(n)n^{-s}$，并设对某个满足$\sigma>\sigma_a$的s，有$F(s)\neq 0$. 那么，存在一个半平面$\sigma>c\geqslant\sigma_a$，$F(s)$在其中恒不为零.

证明　假设没有这样的半平面存在，那么对每一个$K=1, 2, \cdots$，有一个满足$\sigma_k>k$的点s_k，使得$F(s_k)=0$. 因为

当$k\to\infty$时，$\sigma_k\to+\infty$，由唯一性定理得出，对所有的n，有$f(n)=0$，这与$F(s)\neq 0$（对某个s）的假设矛盾.

11.4 Dirichlet级数的乘积

下面的定理把Dirichlet级数的乘积同它们的系数的Dirichlet乘积联系起来.

定理11.15 给定两个由Dirichlet级数表示的函数F(s)与G(s)，

$$F(s)=\sum_{n=1}^{\infty}\frac{f(n)}{n^s}\qquad \text{对}\sigma>a,$$

$$G(s)=\sum_{n=1}^{\infty}\frac{g(n)}{n^s}\qquad \text{对}\sigma>b.$$

则在二级数绝对收敛的半平面里，有

$$(5)\quad F(s)G(s)=\sum_{n=1}^{\infty}\frac{h(n)}{n^s},$$

其中$h=f*g$是f与g的Dirichlet乘积：

$$h(n)=\sum_{d\mid n}f(d)g\left(\frac{n}{d}\right).$$

反之，当$k\to\infty$时，如果$\sigma_k\to+\infty$，对这样的序列$\{s_k\}$里的所有s都有$F(s)G(s)=\sum\alpha(n)n^{-s}$，那么$\alpha=f*g$.

证明　对任一使两个级数都绝对收敛的s，我们有

$$F(s)G(s)=\sum_{n=1}^{\infty}f(n)n^{-s}\sum_{m=1}^{\infty}g(m)m^{-s}$$
$$=\sum_{n=1}^{\infty}\sum_{m=1}^{\infty}f(n)g(m)(mn)^{-s},$$

因为是绝对收敛的，我们能把这两个级数乘在一起，并且可以任何方式重排各项而和不变．把mn是常数的各项集中在一

起并记$mn=k$，k的值能够是1，2，…，于是

$$F(s)G(s)=\sum_{k=1}^{\infty}\left(\sum_{mn=k}f(n)g(m)\right)k^{-s}=\sum_{k=1}^{\infty}h(k)k^{-s},$$

其中$h(k)=\sum_{mn=k}f(n)g(m)=(f*g)(k)$．这证明了第一个断言，而第二个断言由唯一性立即可得． □

例1 两个级数$\sum n^{-s}$与$\sum\mu(n)n^{-s}$对$\sigma>1$都绝对收敛．在(5)式里取$f(n)=1$，$g(n)=\mu(n)$，我们得$h(n)=\left[\frac{1}{n}\right]$，所以

$$\zeta(s)\sum_{n=1}^{\infty}\frac{\mu(n)}{n^s}=1 \qquad \sigma>1.$$

特别，这说明，对$\sigma>1$，$\zeta(s)\neq 0$，并且

$$\sum_{n=1}^{\infty}\frac{\mu(n)}{n^s}=\frac{1}{\zeta(s)} \qquad \sigma>1.$$

例2 更一般，假设$f(1)\neq 0$，并令$g=f^{-1}$为f的Dirichlet逆函数．那么，在两个级数$F(s)=\sum f(n)n^{-s}$与$G(s)=\sum g(n)n^{-s}$都绝对收敛的任一半平面里，我们有$F(s)\neq 0$并且$G(s)=\frac{1}{F(s)}$．

例3 假设$F(s)=\sum f(n)n^{-s}$对$\sigma>\sigma_a$绝对收敛．如果f是完全积性的，那么我们有$f^{-1}(n)=\mu(n)f(n)$．因为$|f^{-1}(n)|\leqslant|f(n)|$，故级数$\sum\mu(n)f(n)n^{-s}$对$\sigma>\sigma_a$也绝对收敛，并且我们有

$$\sum_{n=1}^{\infty}\frac{\mu(n)f(n)}{n^s}=\frac{1}{F(s)} \qquad 当\sigma>\sigma_a时.$$

特别，对任一Dirichlet特征χ，我们有

$$\sum_{n=1}^{\infty}\frac{\mu(n)\chi(n)}{n^s}=\frac{1}{L(s,\chi)} \qquad 当\sigma>1时.$$

例4 取$f(n)=1$，$g(n)=\varphi(n)$为Euler函数. 因为$\varphi(n)\leqslant n$，故级数$\sum\varphi(n)n^{-s}$对$\sigma>2$绝对收敛. 而且，$h(n)=\sum_{d\mid n}\varphi(d)=n$，所以(5)式给出

$$\zeta(s)\sum_{n=1}^{\infty}\frac{\varphi(n)}{n^s}=\sum_{n=1}^{\infty}\frac{n}{n^s}=\zeta(s-1)\quad 当\sigma>2时.$$

因此，

$$\sum_{n=1}^{\infty}\frac{\varphi(n)}{n^s}=\frac{\zeta(s-1)}{\zeta(s)}\qquad 如果\sigma>2.$$

例5 取$f(n)=1$与$g(n)=n^2$，则有$h(n)=\sum_{d\mid n}d^2=\sigma_2(n)$，由(5)式给出

$$\zeta(s)\zeta(s-2)=\sum_{n=1}^{\infty}\frac{\sigma_2(n)}{n^s}$$

若$\sigma>\max\{1,1+R_e(2)\}$.

例6 取$f(n)=1$，$g(n)=\lambda(n)$为Liouville函数，则

$$h(n)=\sum_{n\mid d}\lambda(d)=\begin{cases}1 & 若n=m^2对某个m,\\ 0 & 其它.\end{cases}$$

所以(5)式给出

$$\zeta(s)\sum_{n=1}^{\infty}\frac{\lambda(n)}{n^s}=\sum_{\substack{n=1\\ n=平方数}}^{\infty}\frac{1}{n^s}=\sum_{m=1}^{\infty}\frac{1}{m^{2s}}=\zeta(2s).$$

于是

$$\sum_{n=1}^{\infty}\frac{\lambda(n)}{n^s}=\frac{\zeta(2s)}{\zeta(s)}\quad 当\sigma>1时.$$

11.5 Euler乘积

下面的定理是Euler在1737年发现的，有时称为是算术

基本定理的解析意义.

定理11.6　令f是一个积性数论函数,使得$\sum f(n)$绝对收敛. 那么，这个级数的和能表示为在所有素数上展开的一个绝对收敛的无穷乘积,

$$(6)\quad \sum_{n=1}^{\infty} f(n)=\prod_{p}\{1+f(p)+f(p^2)+\cdots\},$$

如果f是完全积性的，则乘积可简化为

$$(7)\quad \sum_{n=1}^{\infty} f(n)=\prod_{p}\frac{1}{1-f(p)}.$$

注:上面的乘积称为级数的Euler乘积.

证明　考虑在所有素数$p\leqslant x$上展开的有限乘积

$$p(x)=\prod_{p\leqslant x}\{1+f(p)+f(p^2)+\cdots\}.$$

因为这是有限个绝对收敛的级数之积，所以它们可以相乘并可以任一方式重排项的顺序而和不变. 一个有代表性的项是

$$f(p_1^{\alpha_1})f(p_2^{\alpha_2})\cdots f(p_r^{\alpha_r})=f(p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_r^{\alpha_r}),$$

这因为f是积性的. 根据算术基本定理，我们能够写

$$p(x)=\sum_{n\in A}f(n),$$

其次A包含的数n的所有素因数$\leqslant x$，因此,

$$\sum_{n=1}^{\infty} f(n)-p(x)=\sum_{n\in B}f(n),$$

其中B所含的数n至少有一个素因数$>x$，因此

$$\left|\sum_{n=1}^{\infty} f(n)-p(x)\right|\leqslant\sum_{n\in B}|f(n)|\leqslant\sum_{n>x}|f(n)|,$$

因为$\sum|f(n)|$收敛，所以当$x\to\infty$时,上式右端最后的和趋于0. 于是，当$x\to\infty$时，$p(x)\to\sum f(n)$.

当对应的级数$\sum a_n$绝对收敛时，形如$\pi(1+a_n)$的无穷乘

积绝对收敛。此时，我们有

$$\sum_{p\leq x}|f(p)+f(p^2)+\cdots|\leq\sum_{p\leq x}(|f(p)|+|f(p^2)|+\cdots)\leq\sum_{n=2}^{\infty}|f(n)|.$$

因为所有的部分和有界，所以正项级数

$$\sum_{p}|f(p)+f(p^2)+\cdots|$$

收敛，这推出(6)里的乘积绝对收敛。

最后，当f是完全积性函数时，我们有$f(p^n)=f(p)^n$，并且(6)式右端的每一个级数都是收敛的几何级数而其和为$(1+f(p))^{-1}$。 □

对于绝对收敛的Dirichlet 级数应用定理11.6我们立即可得：

定理11.7 **假设$\sum f(n)n^{-s}$对$\sigma>\sigma_a$绝对收敛，如果f是积性函数，则有**

$$(8)\quad \sum_{n=1}^{\infty}\frac{f(n)}{n^s}=\prod_{p}\left\{1+\frac{f(e)}{p^s}+\frac{f(p^2)}{p^{2s}}+\cdots\right\}\quad \text{当}\sigma>\sigma_a\text{时}.$$

如果f是完全积性的，则有

$$\sum_{n=1}^{\infty}\frac{f(n)}{n^s}=\prod_{p}\frac{1}{1+f(p)p^{-s}}\quad \text{当}\sigma>\sigma_a\text{时}.$$

它表明，(8)式里的乘积的一般项是$x=p^{-s}$的函数f的Bell级数$f_p(x)$，(参看2.16节。)

例　分别取$f(n)=1$，$\mu(n)$，$\varphi(n)$，$\sigma_2(n)$，$\lambda(n)$与$\chi(n)$，我们得到下列Euler乘积：

$$\zeta(s)=\sum_{n=2}^{\infty}\frac{1}{n^s}=\prod_{p}\frac{1}{1-p^{-s}}\qquad \text{若}\alpha>1.$$

$$\frac{1}{\zeta(s)}=\sum_{n=1}^{\infty}\frac{\mu(n)}{n^s}=\prod_p(1-p^{-s})\quad 若\sigma>1.$$

$$\frac{\zeta(s-1)}{\zeta(s)}=\sum_{n=1}^{\infty}\frac{\varphi(n)}{n^s}=\prod_p\frac{1-p^{-s}}{1-p^{1-s}}\quad 若\sigma>2.$$

$$\zeta(s)\zeta(s-\alpha)=\sum_{n=1}^{\infty}\frac{\sigma_2(n)}{n^s}=\prod_p\frac{1}{(1-p^{-s})(1-p^{2-s})}$$

$$若\sigma>\max\{1,\ 1+R_e(\alpha)\}.$$

$$\frac{\zeta(2s)}{\zeta(s)}=\sum_{n=1}^{\infty}\frac{\lambda(n)}{n^s}=\prod_p\frac{1}{1+p^{-1}}\quad 若\sigma>1.$$

$$L(s,x)=\sum_{n=1}^{\infty}\frac{\chi(n)}{n^s}=\prod_p\frac{1}{1-\chi(p)p^{-s}}\quad 若\sigma>1.$$

注意，如果$\chi=\chi_1$为模k的主特征，则当$p\mid k$时，$\chi_1(p)=0$，当$p\nmid k$时，$\chi_1(p)=1$，所以$L(s,\ \chi_1)$的Euler乘积为

$$L(s,\ \chi_1)=\prod_p\frac{1}{1-p^{-s}}=\prod_p\frac{1}{1-p^{-s}}\prod_{p\mid k}(1-p^{-s})$$

$$=\zeta(s)\prod_{p\mid k}(1-p^{-s}).$$

即L—函数$L(s,\chi_1)$等于zeta函数乘以有限个因数．

11.6 Dirichlet级数收敛的半平面

为证明收敛半平面的存在性，我们需要利用下面的引理．

引理 2　令$s=\sigma_0+it_0$，并假设Dirichlet级数$\sum f(n)n^{-s_0}$的部分和是有界的，即

$$\left|\sum_{n\leqslant x}f(n)n^{-s_0}\right|\leqslant M$$

对所有$x\geqslant 1$成立．那么对$\sigma>\sigma_0$的每一个s我们有

(9) $\left|\sum_{a<n\leqslant b} f(n)n^{-s}\right| \leqslant 2Ma^{\sigma_0-\sigma}\left(1+\frac{|s-s_0|}{\sigma-\sigma_0}\right)$.

证明 令$a(n)=f(n)n^{-s_0}$并令$A(x)=\sum_{n\leqslant x} a(n)$. 则$f(n)n^{-s}=a(n)n^{s_0-s}$，这样，我们能利用定理4.2($f(x)=x^{s_0-s}$)得到

$$\sum_{a<n\leqslant b} f(n)n^{-s}=A(b)b^{s_0-s}-A(a)a^{s_0-s}$$
$$+(s-s_0)\int_a^b A(t)t^{s_0-s-1}dt.$$

因为$|A(x)|\leqslant M$，所以

$$\left|\sum_{a<n\leqslant b} f(n)n^{-s}\right| \leqslant Mb^{\sigma_0-\alpha}+Ma^{\sigma_0-\sigma}$$
$$+|s-s_0|M\int_a^b t^{\sigma_0-\sigma-1}dt$$
$$\leqslant 2Ma^{\sigma_0-\sigma}+|s-s_0|M\left|\frac{b^{\sigma_0-\sigma}-a^{\sigma_0-\sigma}}{\sigma_0-\sigma}\right|$$
$$\leqslant 2Ma^{\sigma_0-\sigma}\left(1+\frac{|s-s_0|}{\sigma_0-\sigma}\right). \quad \square$$

例 如果部分和$\sum_{n\leqslant x} f(n)$有界，则由引理2推出，对$\sigma>0$，$\sum f(n)n^{-s}$收敛．事实上，如果在(9)里取$s_0=\sigma_0=0$，我们得到，对$\sigma>0$，

$$\left|\sum_{a<n\leqslant b} f(n)n^{-s}\right| \leqslant ka^{-\sigma},$$

其中k对于a是独立的．令$a\to+\infty$，我们得到，当$\sigma>0$时，$\sum f(n)n^{-s}$收敛．特别，这证明了，对$\sigma>0$，Dirichlet级数

$$\sum_{n=1}^{\infty}\frac{(-1)^n}{n^s}$$

收敛，这是因为$\left|\sum_{n\leqslant x}(-1)^n\right|\leqslant 1$．类似地，如果$\chi$是模k的任一非主特征，则我们有$\left|\sum_{n\leqslant x}\chi(n)\right|\leqslant\varphi(k)$，所以

$$\sum_{n=1}^{\infty}\frac{\chi(n)}{n^s}$$

对$\sigma>0$是收敛的．同样的推理可得出下面的定理．

定理11.8　如果级数$\sum f(n)n^{-s}$对$s=\sigma_0+it_0$收敛，那么它对于具有$\sigma>\sigma_0$的所有s收敛．如果它对$s=\sigma_0+it_0$发散，那么它对具有$\sigma<\sigma_0$的所有s发散．

证明　第二个论述可由第一个论述得到．为证明第一个论述，我们选择具有$\sigma>\sigma_0$的任一s，由引理2得出

$$\left|\sum_{a<n<b} f(n)n^{-s}\right|\leqslant ka^{\sigma_0-\sigma},$$

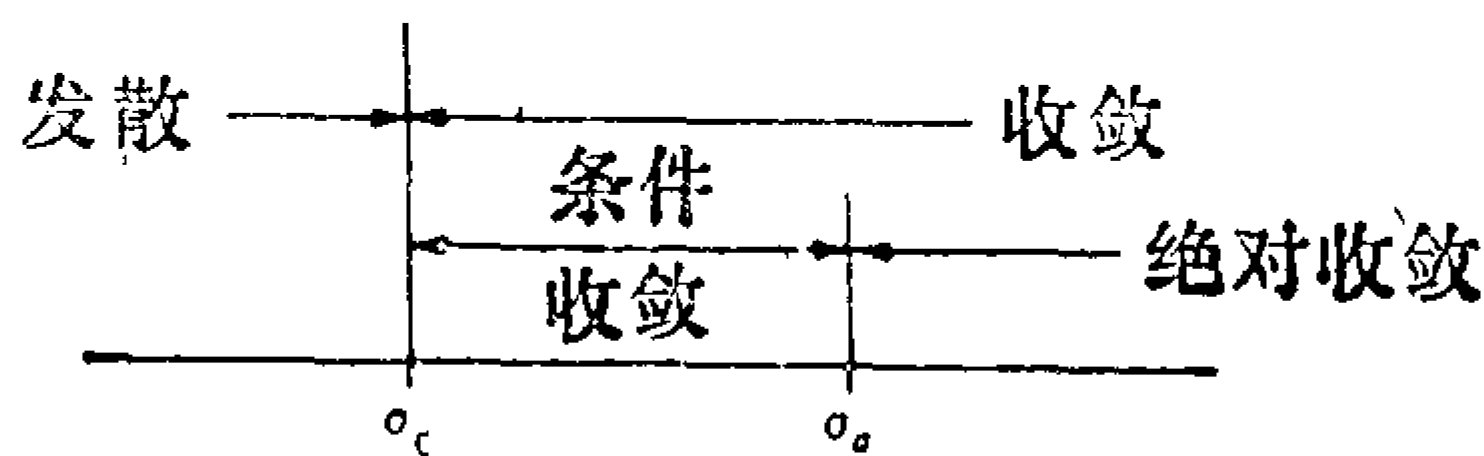
其中k对于a是独立的．因为当$a\to+\infty$时，$a^{\sigma_0-\sigma}\to 0$，由Cauchy判别条件得出$\sum f(n)n^{-s}$收敛．　□

定理11.9　如果级数$\sum f(n)n^{-s}$不是处处收敛或者处处发散，那么存在一个称为收敛横坐标的实数σ_c，使得这个级数在$\sigma>\sigma_c$的半平面里对所有s收敛而在半平面$\sigma<\sigma_c$里对所有s发散．

证明　同定理11.1的证明一样，取σ_c为所有σ的上确界，对$\sigma<\sigma_c$的所有s，$\sum f(n)n^{-s}$发散．

注：如果级数处处收敛，则我们规定$\sigma_c=-\infty$．如果任何地方都不收敛，则我们规定$\sigma_c=+\infty$．

因为绝对收敛也是收敛的，所以我们总有$\sigma_a\geqslant\sigma_c$．如果$\sigma_a>\sigma_c$，则有一个无限的带形区域$\sigma_c<\sigma<\sigma_a$，在它里面，级数条件收敛．（参看图11.1）下面的定理证明，这个带形区域的宽度不超过1．



（图11.1）

定理11.10 对任一σ_c为有限的Dirichlet级数，我们有

$$0 \leqslant \sigma_a - \sigma_c \leqslant 1.$$

证明 我们证明，如果$\sum f(n)n^{-s_0}$对某个s_0收敛，那么对$\sigma > \sigma_0 + 1$的所有s，$\sum f(n)n^{-s}$绝对收敛.

令A是级数$|f(n)n^{-s_0}|$的上界，那么

$$\left|\frac{f(n)}{n^s}\right| = \left|\frac{f(n)}{n^{s_0}}\right|\left|\frac{1}{n^{s-s_0}}\right| \leqslant \frac{A}{n^{\sigma-\sigma_0}}$$

与$\sum n^{\sigma-\sigma_0}$比较，得$\sum|f(n)n^{-s}|$收敛. □

例 如果$\sigma > 0$，则级数

$$\sum_{n=1}^{\infty} \frac{(-1)^n}{n^s}$$

收敛，但只有在$\sigma > 1$时，它才是绝对收敛的. 因此，在这个例子里，$\sigma_c = 0$，$\sigma_a = 1$.

Dirichlet级数收敛的性质可与幂级数比较. 每一个幂级数有一个收敛圆盘，而每一个Dirichlet 级数有一个收敛半平面. 幂级数的收敛圆盘内部也是绝对收敛区域， 而Dirichlet级数的这个绝对收敛区域可以是收敛区域的一个适当的子集合. 一个幂级数在收敛圆盘内部表示一个解析函数，一个Dirichlet 级数在它的收敛半平面内部也表示一个解析函数.

11.7 Dirichlet级数的解析性质

Dirichlet级数的解析性质能由下面的复函数理论的一般定理推出. 这个定理我们表述为一个引理.

引理3 令$\{f_n\}$是一个在复平面的一个开子集上解析的

函数序列，并设$\{f_n\}$在s的任一紧子集上一致收敛于一个函数f，那么f在s上是解析的并且导数序列$\{f_n'\}$在s的任一紧子集上一致收敛于导数f'.

证明　因为f_n在S上是解析的，我们有Cauchy积分公式

$$f_n(a)=\frac{1}{2\pi i}\int_{\partial D}\frac{f_n(z)}{z-a}dz$$

其中D是S里的任一紧圆盘，∂D是它的正向边界，a是D的任一内点。因为一致收敛，我们能得到积分符号下的极限并得

$$f(a)=\frac{1}{2\pi i}\int_{\partial D}\frac{f(z)}{z-a}dz,$$

这说明f在D的世界内是解析的．对于导数，我们有

$$f_n'(a)=\frac{1}{2\pi i}\int_{\partial D}\frac{f_n(z)}{(z-a)^2}dz,$$

$$f'(a)=\frac{1}{2\pi i}\int_{\partial D}\frac{f(z)}{(z-a)^2}dz,$$

由此容易得出，当$n\to\infty$时，在S的任一紧子集上，$f_n'(a)\to f'(a)$，并且是一致收敛的． □

为了对Dirichlet级数应用引理，首先我们指出，Dirichlet级数在它的收敛半平面的紧子集上是一致收敛的．

定理11·11　一个Dirichlet级数$\sum f(n)n^{-s}$在位于收敛半平面$\sigma>\sigma_c$内部的任一紧子集上一致收敛．

证明　若能证明，$\sum f(n)n^{-s}$在任一紧矩形$R=[\alpha,\beta]\times[c,d]$（$\alpha>\sigma_c$）上一致收敛，就足够了．为此，我们利用在引理2里得到的不等式

$$(10)\qquad\left|\sum_{a<n<b}f(n)n^{-s}\right|\leqslant 2Ma^{\sigma_0-\sigma}\left(1+\frac{|S-S_0|}{\sigma-\sigma_0}\right),$$

其中$S_0=\sigma_0+it_0$是半平面$\sigma>\sigma_c$内的任一点，而S是适合$\sigma>\sigma_0$的任一点．我们选取$S_0=\sigma_0$，其中$\sigma_c<\sigma_0<\alpha$．（参看图11.2）



（图11.2）

那么，当$S\in R$时，我们有$\sigma-\sigma_0\geqslant\alpha-\sigma_0$，$|S_0-S|<C$，其中C是依赖于$S_0$的常数而R不依赖于S．则(10)式推出

$$\left|\sum_{a<n\leqslant b} f(n)n^{-s}\right|\leqslant 2Ma^{\sigma_0-\alpha}\left(1+\frac{C}{\alpha-\sigma_0}\right)$$

$$=Ba^{\sigma_0-\alpha}$$

其中B不依赖于S．因为当$a\to+\infty$时，$a^{\sigma_0-\alpha}\to0$，由Cauchy判别条件，唯一性是满足的． □

定理11·12　Dirichlet级数的和函数$F(s)=\sum f(n)n^{-s}$在它的收敛半平面$\delta>\delta_c$上是解析的．并且它的导数$F'(s)$在它的半平面里由Dirichlet级数表示，

$$(11)\quad F'(s)=-\sum_{n=1}^{\infty}\frac{f(n)\log n}{n^s},$$

这由逐项微分而得．

证明　我们对部分和序列应用定理11·11与引理3即得．

注　（11）式里得出的级数$F'(s)$与$F(s)$有相同的收敛横坐标和相同的绝对收敛横坐标．

反复应用定理11·12，我们得到F(s)的k阶导数

$$F^{(k)}(s)=(-1)^k\sum_{n=1}^{\infty}\frac{f(n)(\log n)^k}{n^s}\quad 对\sigma>\sigma_c.$$

例 对$\sigma>1$，我们有

$$(12)\quad \zeta'(s)=-\sum_{n=1}^{\infty}\frac{\log n}{n^s}.$$

与

$$(13)\quad \frac{\zeta'(s)}{\zeta(s)}=\sum_{n=1}^{\infty}\frac{\Lambda(n)}{n^s}.$$

等式(12)由对zeta函数逐项积分而得，(13)是由两个Dirichlet级数$\sum\Lambda(n)n^{-s}$与$\sum n^{-s}$相乘以及利用等式$\sum_{d|n}\Lambda(d)=\log n$而得到.

11.8 具有非负系数的Dirichlet级数

某些由Dirichlet级数确定的函数在它们的收敛半平面$\sigma>\sigma_c$里，除开直线$\sigma=\sigma_c$以外能够是连续解析的. 例如，在下一章，我们将证明Riemann zeta函数$\zeta(s)$除开直线$\sigma=1$以外能够是连续解析的. 这个函数除开一个简单极点$S=1$以外对所有的S都是解析的. 类似地，如果x是一个非主的Dirichlet特征，那么L—函数L(s, x)对一个整数（对所有s解析）除开直线$\sigma=1$以外是连续解析的. 特别地，zeta函数由下面的Landan定理阐明，这个定理论述具有非负系数的Diriehl比级数.

定理11·13 **令F(s)在半平面$\sigma>C$里由Dirichlet级数表示为**

(14) $F(s)=\sum_{n=1}^{\infty}\frac{f(n)}{n^s}$,

其中c是有限的，并且设对所有$n\geqslant n_0$，$f(n)\geqslant 0$. 如果$F(s)$在点$s=c$附近的某个圆内是解析的，那么，对某个$\varepsilon>0$，在半平面$\sigma>c-\varepsilon$里，Dirichlet级数收敛。因而，如果Dirichlet级数有一个收敛的有限横坐标σ_c，那么$F(s)$在实轴上有一个奇点$s=\sigma_c$.

证明　令$a=1+c$. 因为F在a上解析，所以在a附近，它能表示为一个绝对收敛的幂级数展开式，

(15) $F(s)=\sum_{k=0}^{\infty}\frac{F^{(k)}(a)}{k!}(s-a)^k$,

并因F在c上解析，所以这幂级数的收敛半径超过1. (参阅图11.3) 根据定理11.12，导数$F^{(k)}(a)$能由(14)多次微分来确定. 这给我们

$$F^{(k)}(a)=(-1)^k\sum_{n=1}^{\infty}f(n)(\log n)^k n^{-a}$$

所以(15)可改写为

(16) $F(s)=\sum_{k=0}^{\infty}\sum_{n=1}^{\infty}\frac{(a-s)^k}{k!}f(n)(\log n)^k n^{-a}$

因为收敛半径超过1，所以这个公式对某个实数$s=c-\varepsilon$是

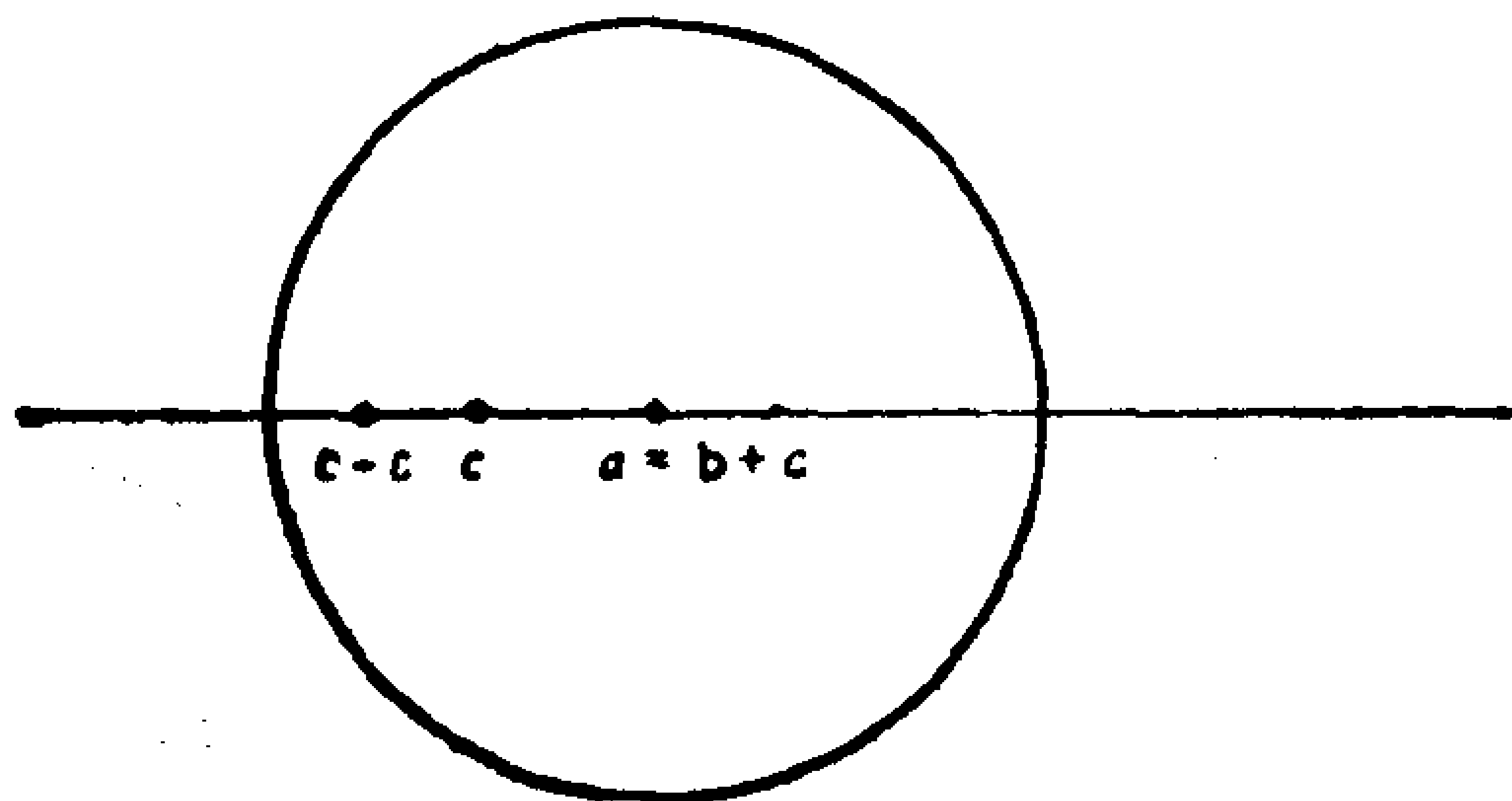


图11.3

正确的，其中$\varepsilon>0$（看图11·3），于是，对这个s，$a-s=1+\varepsilon$，并(16)式里的二重级数对$n\geqslant n_0$有非负的项. 因此我们可以交换求和的顺序而得到

$$F(c-\varepsilon)=\sum_{n=1}^{\infty}\frac{f(n)}{n^a}\sum_{k=0}^{\infty}\frac{\{(1+\varepsilon)\log n\}^k}{k!}$$

$$=\sum_{n=1}^{\infty}\frac{f(n)}{n^a}e^{(1+\varepsilon)\log n}=\sum_{n=1}^{\infty}\frac{f(n)}{n^{c-\varepsilon}}.$$

换言之，对$s=c-\varepsilon$，Dirichlet级数$\sum f(n)n^{-s}$收敛，于是它在半平面$\sigma>c-\varepsilon$里也收敛. □

11.9 Dirichlet级数表示为Dirichlet级数的指数

一个Dirichlet级数$F(s)=\sum f(n)n^{-s}$不恒为0，有一个半平面，在这个半平面里，它决不为0. 下面的定理证明，在这个半平面里，$F(s)$是另一个Dirichlet级数的指数，如果$f(1)\neq 0$.

定理11·14　设$F(s)=\sum f(n)n^{-s}$对于$\sigma>\sigma_a$是绝对收敛的，并假设$f(1)\neq 0$. 对于$\sigma>\sigma_0\geqslant\sigma_a$，如果$F(s)\neq 0$，那么，对于$\sigma>\sigma_0$，我们有

$$F(s)=e^{G(s)},$$

以及

$$G(s)=\log f(1)+\sum_{n=2}^{\infty}\frac{(f'*f^{-1})(n)}{\log n}n^{-s}$$

其中f^{-1}是f的Dirichlet逆函数并且$f'(n)=f(n)\log n$.

注：对于复数$z\neq 0$，$\log z$表示对数的分枝，当$z>0$时，它是实数.

证明　因为$F(s)\neq 0$，所以对某个函数$G(s)$，我们能

够写$F(s)=e^{G(s)}$，对于$\sigma>\sigma_0$，$G(s)$是解析的．求导数，得

$$F'(s)=e^{G(s)}G'(s)=F(s)G'(s),$$

所以$G'(s)=F'(s)/F(s)$．但是

$$F'(s)=-\sum_{n=1}^{\infty}\frac{f(n)\log n}{n^s}=-\sum_{n=1}^{\infty}\frac{f'(n)}{n^s},$$

$$\frac{1}{F(s)}=\sum_{n=1}^{\infty}\frac{f^{-1}(n)}{n^s},$$

于是，

$$G'(s)=F'(s)\frac{1}{F(s)}=-\sum_{n=2}^{\infty}\frac{(f'*f^{-1})(n)}{n^s}.$$

积分，得

$$G(s)=C+\sum_{n=2}^{\infty}\frac{(f'*f^{-1})(n)}{\log n}n^{-s},$$

其中C是常数．令$\sigma\to+\infty$，我们得$\lim_{\sigma\to\infty}G(\sigma+it)=C$于是．

$$f(1)=\lim_{\sigma\to\infty}F(\sigma+it)=e^c,$$

所以$C=\log f(1)$．证明完成．这个证明也得出，当$\sigma>\sigma_0$时，$G(s)$的级数绝对收敛． □

例 1　当$f(n)=1$时，我们有$f'(n)=\log n$，并且$f^{-1}(n)=\mu(n)$，所以

$$(f'*f^{-1})(n)=\sum_{d\mid n}\log d\,\mu\left(\frac{n}{d}\right)=\Lambda(n).$$

因此，如果$\sigma>1$，我们有

(17) $\zeta(s)=e^{G(s)}$，

其中

$$G(s)=\sum_{n=2}^{\infty}\frac{\Lambda(n)}{\log n}n^{-s}.$$

例 2 由类似的理由可证明，如果f是完全可乘的并且$F(s)=\sum f(n)n^{-s}$，那么在绝对收敛的半平面$\sigma>\sigma_a$里，我们有

$$F(s)=e^{G(s)},$$

其中

$$G(s)=\sum_{n=2}^{\infty}\frac{f(n)\Lambda(n)}{\log n}n^{-s},$$

这因为$(f'*f^{-1})(n)=\sum_{d|n}f(d)\log d\mu(n/d)f(n/d)=f(n)\Lambda(n)$.

上面例子中的公式也可借助于Euler乘积推出．例如，对于Riemann zeta函数我们有

$$\zeta(s)=\prod_p\frac{1}{1-p^{-s}},$$

s保持为实数，$s>1$，所以$\zeta(s)$是正的．取对数并利用幂级数$-\log(1-x)=\sum x^m/x$，得

$$\log\zeta(s)=-\sum_p\log(1-p^{-s})=\sum_p\sum_{m=1}^{\infty}\frac{p^{-ms}}{m}$$
$$=\sum_{n=1}^{\infty}\Lambda_1(n)n^{-s},$$

其中

$$\Lambda_1(n)=\begin{cases}\dfrac{1}{m} & \text{若对某个素数}p\text{，有}n=p^m\text{。}\\ 0 & \text{其它.}\end{cases}$$

但是，如果$n=p^m$，那么$\log n=m\log p=m\Lambda(n)$，所以$\frac{1}{m}=\frac{\Lambda(n)}{\log n}$，因此，

$$\log(s)=\sum_{n=2}^{\infty}\frac{\Lambda(n)}{\operatorname{togn}}n^{-s}.$$

这推出(17)式对实数$s>1$成立. 但(17)的每一部分 在半平面$\sigma>1$里是解析的，所以，根据解析石拓性，(17)对$\sigma>1$也成立.

11.10 Dirichlet级数的平均值公式

定理11·15 给定两个Dirichlet级数$F(s)=\sum(n)n^{-s}$与$G(s)=\sum g(n)n^{-1}$，它们分别異有绝对收斂横坐标σ_1与σ_2，那么对于$a>\sigma_1$与$b>\sigma_2$，我们有

$$\lim_{T\to\infty}\frac{1}{2T}\int_{-T}^{T}F(a+it)G(b-it)dt$$
$$=\sum_{n=1}^{\infty}\frac{f(n)g(n)}{n^{a+b}}.$$

证明 我们有

$$F(a+it)G(b-it)=\left(\sum_{m=1}^{\infty}\frac{f(m)}{m^{a+it}}\right)\left(\sum_{n=1}^{\infty}\frac{g(n)}{n^{b-it}}\right)$$
$$=\sum_{\substack{m=1\\ m\neq n}}^{\infty}\sum_{n=1}^{\infty}\frac{f(m)g(n)}{m^a n^b}\left(\frac{n}{m}\right)^{it}$$

于是

$$\sum_{m=1}^{\infty}\sum_{n=1}^{\infty}\left|\frac{f(m)g(n)}{m^a n^b}\left(\frac{n}{m}\right)^{it}\right|$$
$$\leqslant\sum_{m=1}^{\infty}\frac{|f(m)|}{m^a}\sum_{m=1}^{\infty}\frac{|g(n)|}{n^b},$$

所以级数是绝对收敛的，并且收斂性对所以的t 也是 一致性的. 于是我们可逐项积分并用T去除，得

$$\frac{1}{2T}\int_{-T}^{T}F(a+it)G(b-it)dt$$

$$=\sum_{n=1}^{\infty}\frac{f(n)g(n)}{n^{a+b}}+\sum_{\substack{m,n=1\\m\neq n}}^{\infty}\frac{f(m)g(n)}{m^{a}n^{b}}$$

$$\frac{1}{2T}\int_{-T}^{T}e^{it\log\left(\frac{n}{m}\right)}dt$$

但对于$m\neq n$，我们有

$$\int_{-T}^{T}e^{it\log\left(\frac{n}{m}\right)}dt=\left.\frac{e^{it\log\left(\frac{n}{m}\right)}}{i\log\left(\frac{n}{m}\right)}\right|_{-T}^{T}$$

$$=\frac{2\sin\left[T\log\left(\frac{n}{m}\right)\right]}{\log\left(\frac{n}{m}\right)},$$

所以，我们得到

$$\frac{1}{2T}\int_{-T}^{T}F(a+it)G(b-it)dt$$

$$=\sum_{n=1}^{\infty}\frac{f(n)g(n)}{n^{a+b}}+\sum_{\substack{m,n=1\\m\neq n}}^{\infty}\frac{f(m)g(n)}{m^{a}n^{b}}$$

$$\frac{\sin\left[T\log\left(\frac{n}{m}\right)\right]}{T\log\left(\frac{n}{m}\right)}.$$

还有，因为$\frac{(\sin x)}{x}$对x是有界的，所以两个级数对于T是一致收敛的．于是我们通过逐项取极限而得定理结论。

定理11·16　如果$F(s)=\sum_{n=1}^{\infty}f(n)n^{-s}$对$\sigma>\sigma_a$是绝对收敛的，那么对$\sigma>\sigma_a$，我们有

$$(18)\quad \lim_{T\to\infty}\frac{1}{2T}\int_{-T}^{T}|F(\sigma+it)|^2dt=\sum_{n=1}^{\infty}\frac{|f(n)|^2}{n^{2\sigma}}.$$

特别，如果$\sigma>1$，我们有

$$(a)\quad \lim_{T\to\infty}\frac{1}{2T}\int_{-T}^{T}|\zeta(\sigma+it)|^2dt=\sum_{n=1}^{\infty}\frac{1}{n^{2\sigma}}=\zeta(2\sigma).$$

$$(b)\quad \lim_{T\to\infty}\frac{1}{2T}\int_{-T}^{T}|\zeta^{(k)}(\sigma+it)|^2dt=\sum_{n=1}^{\infty}\frac{\log^{2k}n}{n^{2\sigma}}=\zeta^{(2k)}(2\sigma).$$

$$(c)\quad \lim_{T\to\infty}\frac{1}{2T}\int_{-T}^{T}|\zeta(\sigma+it)|^{-2}dt=\sum_{n=1}^{\infty}\frac{u^2(n)}{n^{2\sigma}}=\frac{\zeta(2\sigma)}{\zeta(4\sigma)}.$$

$$(d)\quad \lim_{T\to\infty}\frac{1}{2T}\int_{-T}^{T}|\zeta(\sigma+it)|^4dt=\sum_{n=1}^{\infty}\frac{\sigma_0^2(n)}{n^{2\sigma}}=\frac{\zeta^4(2\sigma)}{\zeta(4\sigma)}.$$

证明　在定理11·15里取$g(n)=\overline{f(n)}$立即得公式(18)．为了推出附加公式(a)到(d)，我们只需对$f(n)$的下列选值求出级数$\sum|f(n)|^2n^{2\sigma}$的值：

(a) $f(n)=1$；(b) $f(n)=(-1)^k\log^k n$；(c) $f(n)=u(n)$；(d) $f(n)=\sigma_0(n)$．公式(a)是显然成立的．公式(b)由关系式

$$\zeta^{(k)}(s)=(-1)^k\sum_{n=1}^{\infty}\frac{\log^k n}{n^s}$$

立即得出．为了证明(c)与(d)，我们利用Euler乘积．对于(c)，我们有

$$\sum_{n=1}^{\infty}\frac{u^2(n)}{n^s}=\prod_p(1+p^{-s})=\prod\frac{1-p^{-2s}}{1-p^{-s}}$$

$$=\frac{\zeta(s)}{\zeta(2s)}.$$

用2σ去代替s，我们就得到(c)．对于(d)，我们写

$$\sum_{n=1}^{\infty}\frac{\sigma_0^2(n)}{n^s}=\prod_p\{1+\sigma_0^2(p)p^{-s}+\sigma_0^2(p^2)p^{-2s}+\cdots\}$$

$$=\prod_p\{1+2^2p^{-s}+3^2p^{-2s}+\cdots\}$$

$$=\prod_p\{\sum(n+1)^2p^{-ns}\}=\prod_p\frac{1-p^{-2s}}{(1-p^{-s})^4}$$

$$=\frac{\zeta^4(s)}{\zeta(2s)}.$$

因为$\sum_{n=0}^{\infty}(n+1)^2x^n=\frac{x+1}{(x-1)^3}=\frac{1-x^2}{(1-x)^4}$，于是用$2\sigma$去代替$s$而得(d)式． □

11.11 Dirichlet级数系数的一个积分公式

定理11·17 **假设级数**$F(s)=\sum_{n=1}^{\infty}f(n)n^{-s}$**对于**$\sigma>\sigma_a$**绝对收敛，那么对于**$\sigma>\sigma_a$**与**$x>0$，**我们有**

$$\lim_{T\to\infty}\frac{1}{2T}\int_{-T}^{T}F(\sigma+it)x^{\sigma+it}dt=\begin{cases}f(n) & \text{若}x=n,\\ 0 & \text{其它}.\end{cases}$$

证明　对于$\sigma>\sigma_a$，我们有

$$(19)\quad \frac{1}{2T}\int_{-T}^{T}F(\sigma+it)x^{\sigma+iT}dt$$

$$=\frac{x^{\sigma}}{2T}\int_{-T}^{T}\sum_{n=1}^{\infty}\frac{f(n)}{n^{\sigma}}\left(\frac{x}{n}\right)^{it}dt$$

$$=\frac{x^{\sigma}}{2T}\sum_{n=1}^{\infty}\frac{f(n)}{n^{\sigma}}\int_{-T}^{T}e^{it\log\left(\frac{x}{n}\right)}dt,$$

因为这个级数对任一区间$[-T,T]$里的所有的t是一致收敛

的．如果x不是一个整数，那么对所有的n，$\frac{x}{n}\neq1$，我们有

$$\int_{-T}^{T}e^{it\log\left(\frac{x}{n}\right)}dt=\frac{2\sin\left[T\log\left(\frac{x}{n}\right)\right]}{\log\left(\frac{x}{n}\right)},$$

级数变为

$$\frac{x^{\sigma}}{T}\sum_{n=1}^{\infty}\frac{f(n)}{n^{\sigma}}\frac{\sin\left[T\log\left(\frac{x}{n}\right)\right]}{\log\left(\frac{x}{n}\right)}$$

当$T\to\infty$时，它趋于0．另一方面，如果x是一个整数，比如$x=k$，那么(19)式里具有$n=k$的项给出

$$\int_{-T}^{T}\left(\frac{x}{n}\right)^{it}dt=\int_{-T}^{T}\left(\frac{k}{k}\right)^{it}dt=\int_{-T}^{T}dt=2T,$$

于是

$$\frac{x^{\sigma}}{2T}\sum_{n=1}^{\infty}\frac{f(n)}{n^{\sigma}}\int_{-T}^{T}\left(\frac{x}{n}\right)^{it}dt$$

$$=f(k)+\frac{k^{\sigma}}{2T}\sum_{\substack{n=1\\n\neq k}}^{\infty}\frac{f(n)}{n^{\sigma}}\int_{-T}^{T}\left(\frac{k}{n}\right)^{it}dt.$$

当$T\to\infty$时，其中第二项趋于0，证明了结论的第一部分． □

11.12 Dirichlet级数部分和的一个积分公式

这一节我们推导出一个把Dirichlet级数的部分和表示为和函数的一个积分的perron公式．我们需要关于围道积分的一个引理．

引理4 如果$c>0$，规定$\int_{c-\infty i}^{c+\infty i}$意指$\lim_{T\to\infty}\int_{c-iT}^{c+iT}$，那么，如果a是任意一个正实数，我们有

$$\frac{1}{2\pi i}\int_{c-\infty i}^{c+\infty i} a^z\frac{dz}{z}=\begin{cases}1 & a若>1\\ \frac{1}{2} & 若a=1\\ 0 & 若a<a<1.\end{cases}$$

此外，我们还有

$$(20)\quad \left|\frac{1}{2\pi i}\int_{c-iT}^{c+iT} a^z\frac{dz}{z}\right|\leqslant\frac{a^c}{\pi T\log\left(\frac{1}{a}\right)}$$

若$0<a<1$，

$$(21)\quad \left|\frac{1}{2\pi i}\int_{c-iT}^{c+iT} a^z\frac{dz}{z}-1\right|\leqslant\frac{a^c}{\pi T\log a}\quad 若a>1,$$

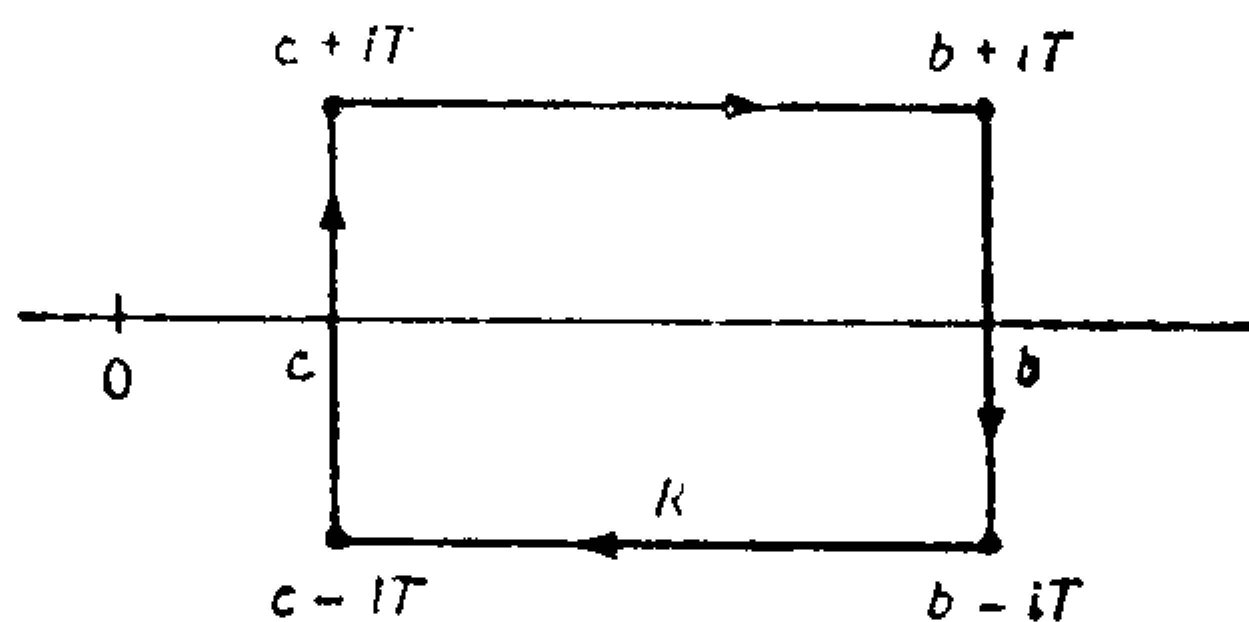
与

$$(23)\quad \left|\frac{1}{2\pi i}\int_{c-iT}^{c+iT}\frac{dz}{z}-\frac{1}{2}\right|\leqslant\frac{c}{\pi T}\quad 若a=1.$$

证明 首先假定$0<a<1$，并考虑图11.4里表示的矩形的周界R. 因为在R内部$\frac{a^z}{z}$是解析的，所以我们有

$\int_R\frac{a^z}{z}dz=0$，于是

$$\int_{c-iT}^{c+iT}=\int_{b+iT}^{c+iT}+\int_{b-iT}^{b+iT}+\int_{c-iT}^{b-iT},$$



（图11.4）

所以

$$\left|\int_{c-iT}^{c+iT} a^z \frac{dz}{z}\right| \leqslant \int_c^b \frac{a^x}{T} dx + \frac{2Ta^b}{b}$$

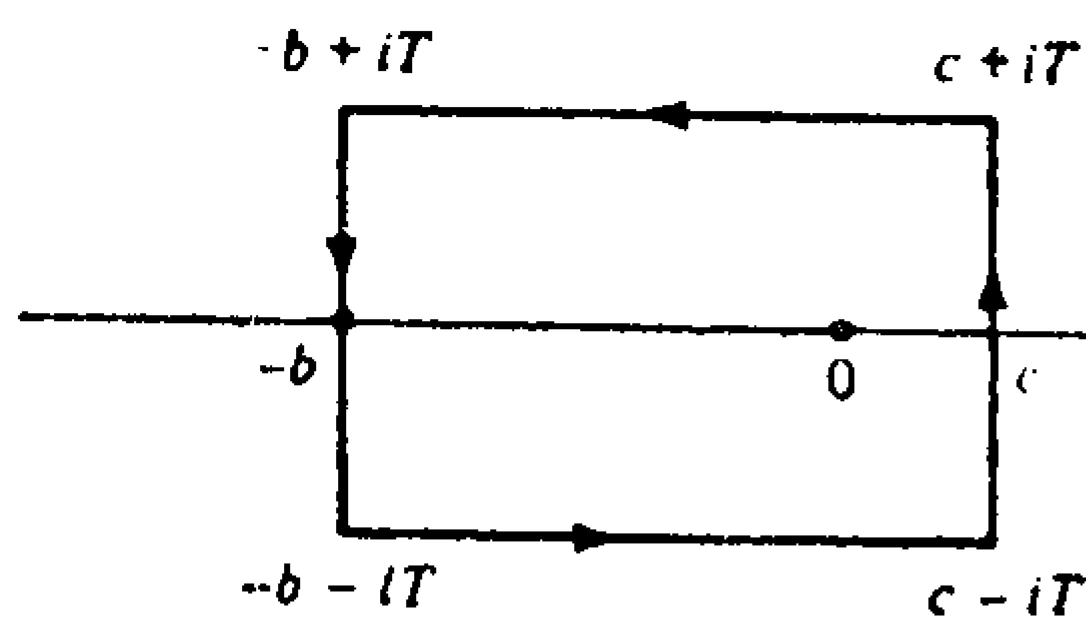
$$+\int_c^b \frac{a^x}{T} dx$$

$$\leqslant \frac{2}{T}\int_c^{\infty} a^x dx + \frac{2Ta^b}{b}$$

$$=\frac{2}{T}\left(\frac{-a^c}{\log a}\right) + \frac{2Ta^b}{b}.$$

令$b\to\infty$，则$a^b\to 0$，于是

$$\left|\int_{c-iT}^{c+iT} a^z \frac{dz}{z}\right| \leqslant \frac{2a^c}{T\log\left(\frac{1}{a}\right)}.$$



（图11.5）

这证明了(20)式.

如果$a>1$，我们就用图11.5里显示的周界代替周界R. 这里$b>c>0$并且$T>c$. 于是$\frac{a^z}{z}$有一个一级极点$z=0$，并有残数1. 因为

$$a^z = e^{z\log a} = 1 + z\log a + 0(|z|^2) \quad \text{当} z\to 0 \text{时}.$$

因此

$$2\pi i = \left(\int_{c-iT}^{c+iT} + \int_{c+iT}^{-b+iT} + \int_{-b+iT}^{-b-iT} + \int_{-b-iT}^{c-iT}\right)$$

$$\times a^z \frac{dz}{z},$$

于是

$$\frac{1}{2\pi i}\int_{c-iT}^{c+iT} a^z\frac{dz}{z}-1=\frac{1}{2\pi i}\left(\int_{-b+iT}^{c+iT}+\int_{-b-iT}^{-b+iT}\right.$$

$$\left.+\int_{c-iT}^{-b-iT}\right)a^z\frac{dz}{z}.$$

现在我们估算右端的积分值，我们有

$$\left|\int_{-b+iT}^{c+iT} a^z\frac{dz}{z}\right|\leqslant\int_{-b}^{c}\frac{a^x dx}{T}\leqslant\frac{1}{T}\int_{-\infty}^{c} a^x dx$$

$$=\frac{1}{T}\frac{a^c}{\log a},$$

$$\left|\int_{-b-iT}^{-b+iT} a^z\frac{dz}{z}\right|\leqslant 2T\frac{a^{-b}}{b},$$

$$\left|\int_{c-iT}^{-b-iT} a^z\frac{dz}{z}\right|\leqslant\int_{-b}^{c}\frac{a^x dx}{T}\leqslant\frac{1}{T}\frac{a^c}{\log a}.$$

当$b\to\infty$时，其中第二个积分趋于0，就得(21)式. 当$a=1$时，我们能直接进行积分. 我们有

$$\int_{c-iT}^{c+iT}\frac{dz}{z}=\int_{T}^{T}\frac{idy}{c+iy}=\int_{-T}^{T}\frac{y}{c^2+y^2}dy$$

$$+ic\int_{-T}^{T}\frac{dy}{c^2+y^2}$$

$$=2ic\int_{0}^{T}\frac{dy}{c^2+y^2}$$

因为被积函数是奇函数，所以其中另一个积分为0. 于是

$$\frac{1}{2\pi i}\int_{c-iT}^{c+iT}\frac{dz}{z}=\frac{c}{\pi}\int_{0}^{T}\frac{dy}{c^2+y^2}=\frac{1}{\pi}\arctan\frac{T}{c}$$

$$=\frac{1}{2}-\frac{1}{\pi}\arctan\frac{c}{T}.$$

因为$\arctan\frac{c}{T}<\frac{c}{T}$，这证明了(22)，并且引理4的证明完成.

定理11.18 Perron公式，令$F(s)=\sum_{n=1}^{\infty}\frac{f(n)}{n^s}$对$\sigma>\sigma_a$是绝对收敛的．又令$c>0$，$x>0$是任意的，那么，当$\sigma>\sigma_a-c$时，我们有

$$\frac{1}{2\pi i}\int_{c-\infty i}^{c+\infty i}F(s+z)\frac{x^z}{z}dz=\sum_{n\leqslant x}^{*}\frac{f(n)}{n^s},$$

其中$\sum^{*}$意指和里最后的项当x是整数时，必须乘以$\frac{1}{2}$.

证明　在积分里，c是z的实部，所以，在半平面$\sigma+c>\sigma_a$的紧子集上，$F(s+z)$的级数是绝对收敛且也是一致收敛的，因此

$$\begin{aligned}&\int_{c-iT}^{c+iT}F(s+z)\frac{x^z}{z}dz\\&=\int_{c-iT}^{c+iT}\sum_{n=1}^{\infty}\frac{f(n)}{n^{s+z}}\times\frac{x^z}{z}dz\\&=\sum_{n=1}^{\infty}\frac{f(n)}{n^s}\int_{c-iT}^{c+iT}\left(\frac{x}{n}\right)^z\frac{dz}{z}\\&=\sum_{n<x}\frac{f(n)}{n^s}\int_{c-iT}^{c+iT}\left(\frac{x}{n}\right)^z\frac{dz}{z}\\&\quad+\sum_{n>x}\frac{f(n)}{n^s}\int_{c-iT}^{c+iT}\left(\frac{x}{n}\right)^z\frac{dz}{z}\\&\quad+'\frac{f(x)}{x^s}\int_{c-iT}^{c+iT}\frac{dz}{z},\end{aligned}$$

符号$+'$表示仅当x是整数时，最后一项才出现．在有限和$\sum_{n<x}$里，我们能够通过对$T\to\infty$逐项取极限，并根据引理4，$\left(其中a=\frac{x}{n},\ a>1\right)$，其积分是$2\pi i$．最后的项（如果它出现的话）得$\pi i f(x)x^{-s}$．如果我们能证明

$$(23)\quad \lim_{T\to\infty}\sum_{n>x}\frac{f(n)}{n^s}\int_{c-iT}^{c+iT}\left(\frac{x}{n}\right)^z\frac{dz}{z}=0,$$

那么定理就得到证明了.

我们知道，当$n>x$时，$\int_{c-i\infty}^{c+i\infty}\left(\frac{x}{n}\right)^z\frac{dz}{z}=0$，但为了证明(23)，在$\int_{c-iT}^{c+iT}$趋于0时，我们必须估算这个式子.

由引理4，我们有估算式

$$\left|\int_{c-iT}^{c+iT}a^z\frac{dz}{z}\right|\leqslant\frac{2}{T}\quad\frac{a^c}{\log\frac{1}{a}}，\text{当}0<a<1\text{ 时.}$$

于是$a=\frac{x}{n}$，$n>x$. 实际上，$n\geqslant[x]+1$，所以，$\frac{1}{a}=\frac{n}{x}\geqslant\frac{([x]+1)}{x}$，于是

$$\left|\sum_{n>x}\frac{f(n)}{n^s}\int_{c-iT}^{c+iT}\left(\frac{x}{n}\right)^z\frac{dz}{z}\right.$$

$$\leqslant\sum_{n>x}\frac{|f(n)|}{n^\sigma}\ \frac{2}{T}\left(\frac{x}{n}\right)^c\frac{1}{\log\left(\frac{[x]+1}{x}\right)}$$

$$=\frac{2}{T}\ \frac{x^c}{\log\left(\frac{[x]+1}{x}\right)}\sum_{n>x}\frac{|f(n)|}{n^{\sigma+c}}\to 0\quad\text{当}T\to\infty$$

时. 这证明了Perron公式. □

注：如果$c>\sigma_a$，则Perron公式对$S=0$是成立的，并且我们得到下面的对于系数的部分和的积分表示：

$$\frac{1}{2\pi i}\int_{c-\infty i}^{c+\infty i}F(z)\ \frac{x^z}{z}\ dz=\sum_{n\leqslant x}^{*}f(n).$$

第十一章习题

1. 推导下列等式对$\sigma>1$成立.

(a) $\zeta(s)=s\int_1^{\infty}\frac{[x]}{x^{s+1}}dx$.

(b) $\sum_p\frac{1}{p^s}=s\int_1^{\infty}\frac{\pi(x)}{x^{s+1}}dx$，其中和式在所有素数上展开.

(c) $\frac{1}{\zeta(s)}=s\int_1^{\infty}\frac{M(x)}{x^{s+1}}dx$，其中$M(x)=\sum_{n\leqslant x}u(n)$.

(d) $-\frac{\zeta'(s)}{\zeta(s)}=s\int_1^{\infty}\frac{\psi(x)}{x^{s+1}}dx$，其中$\psi(x)=\sum_{n\leqslant x}\Lambda(n)$.

(e)$l(s, x)=s\int_1^{\infty}\frac{A(x)}{x^{s+1}}dx$，其中$A(x)=\sum_{n\leqslant x}x(n)$.

如果x是非主特征，证明(e)对$\sigma>0$也成立. [提示：定理4.2]

2. 假设级数$\sum_{n=1}^{\infty}f(n)$收敛,其和为A,并令$A(x)=\sum_{n\leqslant x}f(n)$.

(a) 证明Dirichlet级数$F(s)=\sum_{n=1}^{\infty}f(n)n^{-s}$对每个s与$\sigma>0$收敛，并且

$$\sum_{n=1}^{\infty}\frac{f(n)}{n^s}=A-S\int_1^{\infty}\frac{R(x)}{x^{s+1}}dx,$$

其中$R(x)=A-A(x)$. [提示：定理4.2]

(b) 推证$F(\sigma)\to A$，当$\sigma\to 0+$时.

(c) 如果$\sigma>0$，并且$N\geqslant1$是整数，证明

$$F(s)=\sum_{n=1}^{N}\frac{f(n)}{n^s}-\frac{A(N)}{N^s}+s\int_N^{\infty}\frac{A(y)}{y^{s+1}}dy.$$

(d) 写$s=\sigma+it$，在(c)里取$N=1+[|t|]$，证明

$|F(\sigma+it)|=O(|t|^{1-\sigma})$　当$0<\sigma<1$时.

3. (a) 证明级数$\sum n^{-1-it}$　当$t\neq 0$时部分和有界，当$t=0$时部分和无界.

(b) 证明级数$\sum n^{-1-it}$对所有实数发散．换言之，$\zeta(s)$的Dirichlet级数在直线$\sigma=1$上处处发散.

4. 令$F(s)=\sum_{n=1}^{\infty}f(n)n^{-s}$，其中$f(n)$是完全积性的，并且级数对$\sigma>\sigma_a$绝对收敛．证明，如果$\sigma>\sigma_a$，则我们有

$$\frac{F'(s)}{F(s)}=-\sum_{n=1}^{\infty}\frac{f(n)\Lambda(n)}{n^s}.$$

在下列习题里，$\lambda(n)$是Liouville函数，$d(n)$是n的约数的个数，$v(n)$与$k(n)$定义如下：$v(1)=0$，$k(1)=1$；如果$n=P_1^{\alpha_1}\cdots P_k^{\alpha_k}$，则$v(n)=k$，$k(n)=\alpha_1\alpha_2\cdots\alpha_k$.

证明 5 至10题里的等式对$\sigma>1$是成立的.

5. $\displaystyle\sum_{n=1}^{\infty}\frac{d(n^2)}{n^s}=\frac{\zeta^3(s)}{\zeta(2s)}.$

6. $\displaystyle\sum_{n=1}^{\infty}\frac{v(n)}{n^s}=\zeta(s)\sum_{P}\frac{1}{P^s}.$

7. $\displaystyle\sum_{n=1}^{\infty}\frac{2^{v(n)}}{n^s}=\frac{\zeta^2(s)}{\zeta(2s)}.$

8. $\displaystyle\sum_{n=1}^{\infty}\frac{2^{v(n)}\lambda(n)}{n^s}=\frac{\zeta(2s)}{\zeta^2(s)}.$

9. $\displaystyle\sum_{n=1}^{\infty}\frac{k(n)}{n^s}=\frac{\zeta(s)\zeta(2s)\zeta(3s)}{\zeta(6s)}.$

10. $\displaystyle\sum_{n=1}^{\infty}\frac{3^{v(n)}k(n)}{n^s}=\frac{\zeta^3(s)}{\zeta(3s)}.$

11．用Riemann zeta函数表示级数和$\sum_{n=1}^{\infty}3^{\nu(n)}k(n)\lambda(n)\times n^{-s}$．

12．设f是完全积性函数，使得对每一个素数p，有$f(p)=f(p)^2$．如果级数$\sum f(n)n^{-s}$对$\sigma>\sigma_a$绝对收敛并且和为F(s)，证明$F(s)\neq 0$，并且证明

$$\sum_{n=1}^{\infty}\frac{f(n)\lambda(n)}{n^s}=\frac{F(2s)}{F(s)}，若\sigma>\sigma_a$$

13． 令f是一个积性函数，使得对每一个素数P，有$f(p)=f(p)^2$．如果级数$\sum u(n)f(n)n^{-s}$对$\sigma>\sigma_a$绝对收敛并且和为F(s)，证明$F(s)\neq 0$并且

$$\sum_{n=1}^{\infty}\frac{f(n)|u(n)|}{n^s}=\frac{F(2s)}{F(s)}，若\sigma>\sigma_a$$

14．令f是一个积性函数，使得对$\sigma>\sigma_a$，$\sum f(n)n^{-3}$绝对收敛．如果P是素数并且$\sigma>\sigma_a$，证明

$$(1+f(p)p^{-s})\sum_{n=1}^{\infty}\frac{f(n)\mu(n)}{n^s}$$
$$=(1-f(p)p^{-s}\sum_{n=1}^{\infty}\frac{f(n)\mu(n)\mu(p,n)}{n^s},$$

其中$\mu(p,n)$是Möbius函数在p与n的最大公约数上的值．
[提示：Ealer乘积．]

15．证明

$$\sum_{m=1}^{\infty}\sum_{\substack{n=1\\(m,n)=1}}^{\infty}\frac{1}{m^2n^2}=\frac{\zeta^2(2)}{\zeta(4)}.$$

更一般，如果每一个s_i的实部$\sigma_i>1$，用Riemann zeta函数表示乘积和

$$\sum_{\substack{m_1=1\\(m_1,\cdots,m_r)=1}}^{\infty}\cdots\sum_{m_r=1}^{\infty}m_1^{-s_1}\cdots m_r^{-s_r}.$$

16. 积分

$$(24)\quad f(s)=\int_1^{\infty}\frac{A(x)}{x^s}dx,$$

其中$A(x)$在任一紧区间$[1, a]$里是Riemann可积的，这种积分的某些性质与Dirichlet级数的性质相似．例如，它们有一个绝对收敛的半平面$\sigma>\sigma_a$与一个收敛半平面$\sigma>\sigma_c$，在这里面$f(s)$是解析的．这个习题的描述与定理11.13类似(Landau定理)．令$f(s)$是根据(24)在半平面$\sigma>\sigma_c$里表示的函数，其中σ_c是有限的．并且假设$A(x)$是实值的并对$x\geqslant x_0$不改变符号．证明$f(s)$在实轴上有一个奇点$s=\sigma_c$.

17. 令$\lambda_a(n)=\sum_{d\mid n}d^a\lambda(d)$，其中$\lambda(n)$是Liouill函数．证明，如果$\sigma>\max\{1, \mathrm{Re}(a)+1\}$，则我们有

$$\sum_{n=1}^{\infty}\frac{\lambda_a(n)}{n^s}=\frac{\zeta(s)\zeta(2s-2a)}{\zeta(s-a)}$$

和

$$\sum_{n=1}^{\infty}\frac{\lambda(n)\lambda_a(n)}{n^s}=\frac{\zeta(2s)\zeta(s-a)}{\zeta(s)}.$$

第十二章　函数$\zeta(s)$和$L(s,\chi)$

12.1　引言

这一章我们逐步讨论Riemann zeta函数$\zeta(s)$与Dirichlet L—函数$L(s,\chi)$的更进一步的性质．对于$\sigma>1$，这两个级数为

$$\zeta(s)=\sum_{n=1}^{\infty}\frac{1}{n^s},\quad L(s,\chi)=\sum_{n=1}^{\infty}\frac{\chi(n)}{n^s}.$$

同上一章一样，我们记$s=\sigma+it$．$\zeta(s)$与$L(s,\chi)$能用Hurwitz zeta函数$\zeta(s,a)$统一起来．对于$\sigma>1$，$\zeta(s,a)$由级数

$$\zeta(s,a)=\sum_{n=0}^{\infty}\frac{1}{(n+a)^s}$$

定义　这里a是一个固定的实数，$0<a\leqslant1$．当$a=1$时，这个函数简化为Riemann zeta函数$\zeta(s)=\zeta(s,1)$．我们也能用Hurwitz zeta函数来表示$L(s,\chi)$．如果χ是模k的一个特征，我们按模k的剩余类来重排$L(s,\chi)$的级数里项的顺序．我们写

$n=qk+r$　其中$1\leqslant r\leqslant k$，$q=0,1,2\cdots$，

得

$$L(s, x)=\sum_{n=1}^{\infty}\frac{x(n)}{n^s}=\sum_{r=1}^{\infty}\sum_{q=0}^{\infty}\frac{x(qk+r)}{(qk+r)^s}$$

$$=\frac{1}{k^s}\sum_{r=1}^{k}x(r)\sum_{q=0}^{\infty}\frac{1}{\left(q+\frac{r}{k}\right)^s}$$

$$=k^{-s}\sum_{r=1}^{k}x(r)\zeta\left(s, \frac{r}{k}\right).$$

这就把$L(s, x)$表示为Hurwitz zeta函数的一个线性组合，这样，L—函数的性质最终依赖$\zeta(s, a)$的性质而定.

我们的首要目标是在直线$\sigma=1$之外，$\zeta(s, a)$解析开拓.这要由gamma函数$\Gamma(s)$的积分公式去得到$\zeta(s, a)$的积分表示式才能达到目标.

12.2 gamma函数的性质

整个这一章我们将需要gamma函数$\Gamma(s)$的一些基本性质.这些性质列举如下以便于参考.虽然不是全部性质但都是必需的.这些性质的证明是大多数复函数论教科书的基础.

对于$\sigma>0$，我们有积分表示式

(1) $\Gamma(s)=\int_0^{\infty}x^{s-1}e^{-x}dx.$

对于$\sigma>0$，这样定义的函数在直线$\sigma=0$之外是连续的，$\Gamma(s)$作为一个函数存在，在s平面里，它是处处解析的，除开一些简单极点

$$s=0,\ -1,\ -2,\ -3\ \cdots$$

之外.在$s=-n$时，具有残数$\frac{(-1)^n}{n!}$.我们还有表示式

$$\Gamma(s)=\lim_{n\to\infty}\frac{n^s n!}{s(s+1)\cdots(s+n)}$$

对$s\neq 0$，-1，$-2\cdots$.

与乘积公式

$$\frac{1}{\Gamma(s)}=se^{cs}\prod_{n=1}^{\infty}\left(1+\frac{s}{n}\right)e^{\frac{-s}{n}}\text{对所有}s,$$

其中c是Euler常数．因为这个乘积对所有S收敛，所以$\Gamma(s)$决不为0．gamma函数还满足两个函数等式，

（2）$\Gamma(s+1)=S\Gamma(s)$

和

（3）$\Gamma(s)\Gamma(1-s)=\frac{\pi}{\sin\pi s}$,

对所有s成立．乘法公式

（4）$\Gamma(s)\Gamma\left(s+\frac{1}{m}\right)\cdots\Gamma\left(s+\frac{m-1}{m}\right)=(2\pi)^{\frac{(m-1)}{2}}$

$\times m^{\left(\frac{1}{2}\right)-ms}\Gamma(ms)$，对所有s及所有整数$m\geq 1$成立．

我们将用到积分表示式（1），函数等式（2）和（3），以及$\Gamma(s)$在整个平面存在的事实．在整数$s=0$，-1，-2，$\cdots$ $\Gamma(s)$有简单极点．如果n是一个非负整数，我们还注意$\Gamma(n+1)=n!$.

12.3 Hurwitz zeta函数的积分表示

对$\sigma>1$，Hurwitz zeta函数是由级数

$$\zeta(s,\ a)=\sum_{n=0}^{\infty}\frac{1}{(n+a)^s}$$

定义的，这在本章开始时已经给出．

定理12.1　对$\sigma>1$，$\zeta(s,\ a)$的级数是绝对收敛的．这个收敛性在任一半平面$\sigma\geqslant 1+\delta$，$\delta>0$里还是一致的．所以$\zeta(s,\ a)$在半平面$\sigma>1$里是s的一个解析函数．

证明　所有这些结论可由下面的不等式得到．

$$\sum_{n=1}^{\infty}|(n+a)^{-s}|=\sum_{n=1}^{\infty}(n+a)^{-\sigma}\leqslant\sum_{n=1}^{\infty}(n+a)^{-(1+\delta)}$$

□

定理12.2　对$\sigma>1$，我们有积分表示式

$$(5)\quad \Gamma(s)\zeta(s,\ a)=\int_0^{\infty}\frac{x^{s-1}e^{-ax}}{1-e^{-x}}dx.$$

特别，当$a=1$时，我们有

$$\Gamma(s)\zeta(s)=\int_0^{\infty}\frac{x^{s-1}e^{-x}}{1-e^{-x}}dx.$$

证明　首先我们保持s为实数，$s>1$，然后根据解析开拓把这个结果扩大到复数s．

在$\Gamma(s)$的积分表示式里，我们做变量替换$x=(n+at)$，其中$n\geqslant 0$，得

$$\Gamma(s)=\int_0^{\infty}e^{-x}x^{s-1}dx=(n+a)^s\int_0^{\infty}e^{-(n+a)t}t^{s-1}dx$$

或者

$$(n+a)^{-s}\Gamma(s)=\int_0^{\infty}e^{-nt}e^{-at}t^{s-1}dt.$$

对所有的$n\geqslant 0$求和，我们得

$$\zeta(s,\ a)\Gamma(s)=\sum_{n=0}^{\infty}\int_0^{\infty}e^{-nt}e^{-at}t^{s-1}dt,$$

如果$\sigma>1$，则右边的级数收敛．现在我们希望把和与积分的顺序交换，最简单的方法是证明这个积分可以看作是 Lebe-

sgue积分．因为被积函数是非负的，Levi收敛性定理（参考〔2〕里定理10.25）告诉我们，级数

$$\sum_{n=0}^{\infty} e^{-nt}e^{-at}t^{s-1}$$

几乎处处收敛于和函数，这个和函数在〔0，$+\infty$〕上是Lebesgue—可积函数．并且

$$\zeta(s,\ a)\ \Gamma(s)=\sum_{n=0}^{\infty}\int_0^{\infty} e^{-nt}e^{-at}t^{s-1}\,dt$$

$$=\int_0^{\infty}\sum_{n=0}^{\infty} e^{-nt}e^{-at}e^{s-1}dt.$$

但若$t>0$，则我们有$0<e^{-t}<1$，于是

$$\sum_{n=0}^{\infty} e^{-nt}=\frac{1}{1-e^{-t}},$$

因为这个级数是一个几何级数．因此，我们有

$$\sum_{n=0}^{\infty} e^{-nt}e^{-at}t^{s-1}=\frac{e^{-at}t^{s-1}}{1-e^{-t}},$$

它在〔0，$+\infty$〕几乎处处成立．实际上，除0以外，是处处成立的．所以

$$\zeta(s,\ a)\Gamma(s)=\int_0^{\infty}\sum_{n=0}^{\infty} e^{-nt}e^{-at}t^{s-1}\,dt$$

$$=\int_0^{\infty}\frac{e^{-at}t^{s-1}}{1-e^{-t}}dt.$$

这证明了(5)式对实数$s>1$成立．为了把它扩大为对所有实数s及$\sigma>1$都成立，我们注意，等式两边对$\sigma>1$是解析的．为了证明右边部分是解析的，我们假设$1+\delta\leqslant\sigma\leqslant c$，其中$c>1$，$\delta>0$，并写

$$\int_0^{\infty}\left|\frac{e^{-at}t^{s-1}}{1-e^{-t}}\right|dt\leqslant\int_0^{\infty}\frac{e^{-at}t^{\sigma-1}}{1-e^{-t}}\,dt$$

$$=\left(\int_0^1+\int_1^{\infty}\right)\frac{e^{-at}t^{\sigma-1}}{1-e^{-t}}dt.$$

如果$0\leqslant t\leqslant 1$，我们有$t^{\sigma-1}\leqslant t^{\delta}$，又若$t\geqslant 1$，则我们有$t^{\sigma-1}$
$\leqslant t^{c-1}$．还因为对$t\geqslant 0$，有$e^{t}-1$，所以有

$$\int_0^1\frac{e^{-at}t^{\sigma-1}}{1-e^{-t}}dt\leqslant\int_0^1\frac{e^{(1-a)t}t^{\delta}}{e^{t}-1}dt$$

$$\leqslant e^{1-a}\int_0^1 t^{\delta-1}dt=\frac{e^{1-a}}{\delta},$$

与

$$\int_1^{\infty}\frac{e^{-at}t^{\sigma-1}}{1-e^{-t}}dt\leqslant\int_1^{\infty}\frac{e^{-at}t^{c-1}}{1-e^{-t}}dt$$

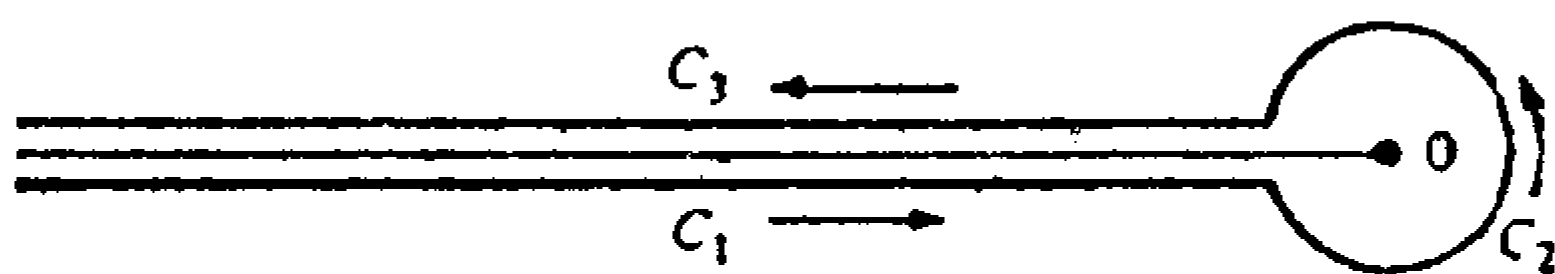
$$\leqslant\int_0^{\infty}\frac{e^{-at}t^{c-1}}{1-e^{-t}}dt$$

$$=\Gamma(c)\zeta(c,\ a).$$

这说明(5)式里的积分在每一个带形区域$1+\delta\leqslant\delta\leqslant c$里是一致收敛的，其中$\delta>0$．因此在每一个这样的带形里，因而也在半平面$\sigma>1$里，描述了一个解析函数．于是，根据解析开拓，在$\sigma>1$时，(5)式对所有s成立． □

12.4 Hurwitz zeta函数的围道积分表示

为了在直线$\sigma=1$之外展开$\zeta(s,\ a)$，我们用围道积分来推出$\zeta(s,\ a)$的另一种表示法．围道c在负实轴周围是一个回环，如图12.1所示．这个回环由c_1，c_2，c_3三部分组成．c_2是在原点周围的半径$c<2\pi$的一个正向圆．而c_1与c_3是z一平面上沿着负实轴的下边缘与上边缘来回移动的一条“割线”．如图12.1所示．



（图12.1）

这就是说，我们利用参数化方法，在c_1上有$z=re^{-\pi i}$，在c_3上有$z=re^{\pi i}$，其中r由c变到$+\infty$.

定理12.3　如果$0<a<1$，由围道积分定义的函数

$$I(s,a)=\frac{1}{2\pi i}\int_c \frac{z^{s-1}e^{az}}{1-e^{z}}dz$$

是s的一个整函数，此外，我们还有

(6) $\zeta(s,a)=\Gamma(1-s)I(s,a)$　**当$\sigma>1$时.**

证明　在c_1上z^s就是$r^s e^{-\pi i s}$，而在c_3上z^s就是$r^s e^{\pi i s}$. 我们考虑一个紧的圆面$|s|\leqslant M$，并证明在每一个这样的圆上沿c_1与c_3的积分一致收敛. 因为被积函数是s的一个整函数，这能证明$I(s,a)$也是一个整函数.

沿着c_1，对$r\geqslant 1$，我们有

$$|z^{s-1}|=r^{\sigma-1}|e^{-\pi i(\sigma-1+it)}|$$
$$=r^{\sigma-1}e^{\pi t}\leqslant r^{M-1}e^{\pi M},$$

这因为$|s|\leqslant M$. 类似地，沿着c_3，对$r\geqslant 1$，我们有

$$|z^{s-1}|=r^{\sigma-1}|e^{\pi i(\sigma-1+it)}|=r^{\sigma-1}e^{-\pi t}\leqslant r^{M-1}e^{\pi M}.$$

于是，在c_1或c_3之任何一个上，对$r\geqslant 1$，我们有

$$\left|\frac{z^{s-1}e^{az}}{1-e^{z}}\right|\leqslant\frac{r^{M-1}e^{\pi M}e^{-ar}}{1-e^{-r}}=\frac{r^{M-1}e^{\pi M}e^{(1-a)r}}{e^{r}-1}.$$

但是，当$r>\log 2$时，$e^r-1>\frac{e^r}{2}$，所以被积函数不超过$Ar^{M-1}e^{-ar}$，其中A是一个依赖于M的常数，但它与r无关.

因为$\int_c^{\infty} r^{M-1}e^{-ar}dr$在$c>0$时收敛，这表明，在每一个紧圆$|s|\leqslant M$上，沿$c_1$与$c_3$，积分一致收敛. 于是$I(s, a)$是S的一个整函数.

为证明(6)，我们写

$$2\pi i I(s, a)=\left(\int_{c_1}+\int_{c_2}+\int_{c_3}\right)z^{s-1}g(z)dz$$

其中$g(z)=\frac{e^{az}}{(1-e^z)}$. 在$c_1$与$c_3$上我们有

$g(z)=g(-r)$，在c_2上我们写$z=ce^{i\theta}$，其中$-\pi\leqslant\theta\leqslant\pi$，这给出

$$\begin{aligned}2\pi i I(s, a)=&\int_{+\infty}^{c} r^{s-1}e^{-\pi i s}g(-r)dr\\&+i\int_{-\pi}^{\pi} c^{s-1}e^{(s-1)i\theta}ce^{i\theta}g(ce^{i\theta})d\theta\\&+\int_c^{\infty} r^{s-1}e^{\pi i s}g(-r)dr\\=&2i\sin(\pi s)\int_c^{\infty} r^{s-1}g(-r)dr\\&+ic^s\int_{-\pi}^{\pi} e^{is\theta}g(ce^{i\theta})d\theta.\end{aligned}$$

用2i去除，得

$$\pi I(s, a)=\sin(\pi s)I_1(s, c)+I_2(s, c),$$

令$c\to 0$，得

$$\lim_{c\to 0} I(s, c)=\int_0^{\infty}\frac{r^{s-1}e^{-ar}}{1-e^{-r}}dr=\Gamma(s)\zeta(s, a),$$

如果$\sigma>1$的话，下面我们证明$\lim\limits_{c\to 0} I_2(s, c)=0$.

为此，注意$g(z)$除开一级极点$z=0$之外，在$|z|\leqslant 2\pi$内是解析的. 因此$zg(z)$在$|z|\leqslant 2\pi$内是处处解析的. 于是$|g(z)|$

$\leqslant \frac{A}{|z|}$是有界的．其中$|z|=c<2\pi$并且A是一个常数．因此，我们有

$$|I_2(s,\ c)|\leqslant\frac{c^\sigma}{2}\int_{-\pi}^{\pi}e^{-t\theta}\frac{A}{c}d\theta\leqslant Ae^{\pi|t|}c^{\sigma-1}.$$

如果$\sigma>1$，$c\to0$，我们得到$I_2(s,\ c)\to0$，于是$\pi I(s,\ a)=\sin(\pi s)\Gamma(s)\zeta(s,\ a)$．因为$\Gamma(s)\Gamma(1-s)=\frac{\pi}{\sin\pi s}$，这证明(6)成立．□

12.5 Hurwitz zeta函数的解析开拓

等式$\zeta(s,\ a)=\Gamma(1-s)I(s,\ a)$对$\sigma>1$成立．其中函数$I(s,\ a)$与$\Gamma(1-s)$对每一个复数$c$有意义．因此，对$\sigma\leqslant1$我们能利用这个等式去定义$\zeta(s,\ a)$．

定义　如果$\sigma\leqslant1$，我们根据等式

(7) $\zeta(s,\ a)=\Gamma(1-s)I(s,\ a)$

定义$\zeta(s,\ a)$．这个等式说明，在整个平面里，$\zeta(s,\ a)$是解析的．

定理12.4　如上定义的函数$\zeta(s,\ a)$，除开一个残数为1的简单极点$s=1$之外，对所有s都是解析的．

证明　因为$I(s,a)$是整函数，所以$\Gamma(1-s)$的极点$s=1$，2，3，…是$\zeta(s,\ a)$仅有的可能的极点．但定理12.1证明了$\zeta(s,\ a)$在$s=2$，3，…上是解析的，所以$s=1$是$\zeta(s,a)$的唯一可能的极点．

现在我们证明$s=1$是具有残数1的一个极点．如果s是任意整数，比如$s=n$，在$I(s,\ a)$的围道积分里被积函数在

c_1与c_3上取相同的值，于是消去沿c_1与c_3的积分，剩下

$$I(n, a)=\frac{1}{2\pi i}\int\frac{z^{n-1}e^{az}}{1-e^z}dz=\operatorname*{Res}_{z=0}\frac{z^{n-1}e^{az}}{1-e^z}.$$

特别，当$s=1$时，我们有

$$I(1, a)=\operatorname*{Res}_{z=0}\frac{e^{az}}{1-e^z}=\lim_{z\to 0}\frac{ze^{az}}{1-e^z}=\lim_{z\to 0}\frac{-1}{e^z}$$
$$=-1.$$

为了得到在$s=1$处$\zeta(s, a)$的残数，我们计算极限

$$\lim_{s\to 1}(s-1)\zeta(s, a)=-\lim_{s\to 1}(1-s)\Gamma(1-s)I(s, a)$$
$$=-I(1, a)\lim_{s\to 1}\Gamma(2-s)$$
$$=\Gamma(1)=1.$$

这证明$\zeta(s, a)$有一个残数为1的简单极点$s=1$.

注：因为$\zeta(s, a)$在$s=2$，3…上是解析的，而在这些点上$\Gamma(1-s)$有极点，由等式(7)得出$I(s, a)$在这些点上为零.

12.6 $\zeta(s)$与$L(s,x)$的解析开拓

在章引言里我们证明了，对$\sigma>1$我们有

$$\zeta(s)=\zeta(s, 1)$$

与

$$(8)\quad L(s, x)=K^{-s}\sum x(r)\zeta\left(s, \frac{r}{k}\right),$$

其中x是模k的任一Dirichlet特征．现在我们用这两个公式作为函数$\zeta(s)$与$L(s, x)$的定义，对$\sigma\leqslant 1$．用这种方法我们得到在直线$\sigma=1$之外，$\zeta(s)$与$L(s, x)$的解析开拓性.

定理12.5

(a) **Riemann zeta函数除开一个残数为1的简单极点**

$s=1$之外，是处处解析的.

(b) 对于主特征$\chi_1 \bmod k$，L—函数$L(s,\chi_1)$除开一个残数为$\frac{\varphi(k)}{k}$的简单极点$s=1$之外，是处处解析的.

(c) 如果$\chi \neq \chi_1$，则$L(s, \chi)$是s的整函数.

证明 由定理12.4立即可得(a). 为证明(b)与(c)，我们利用关系式

$$\sum_{r \bmod k} \chi(r) = \begin{cases} 0 & 若\chi \neq \chi_1 \\ \varphi(k) & 若\chi = \chi_1. \end{cases}$$

因为$\zeta\left(s, \frac{r}{k}\right)$有一个残数为1的简单极点$s=1$，所以函数$\chi(r)\zeta\left(s, \frac{r}{k}\right)$有一个残数为1的简单极点$s=1$. 因此

$$\begin{aligned} \operatorname*{Res}_{s=1} L(s, \chi) &= \lim_{s \to 1}(s-1)L(s, \chi) \\ &= \lim_{s \to 1}(s-1)k^{-s}\sum_{r=1}^{k} \chi(r)\zeta\left(s, \frac{r}{k}\right) \\ &= \frac{1}{k}\sum_{r=1}^{k}\chi(r) = \begin{cases} 0 & 若\chi \neq \chi_1, \\ \frac{\varphi(k)}{k} & 若\chi = \chi_1. \end{cases} \end{aligned}$$

□

12.7 $\zeta(s,a)$的Hurwitz公式

函数$\zeta(s, a)$对$\sigma>1$有一个由无穷级数表示的初始定义. Hurwitz得到$\zeta(s, a)$的另一个级数表示式，它在半平面$\sigma<0$里是正确的. 这个公式的证明将要用到下面的引理.

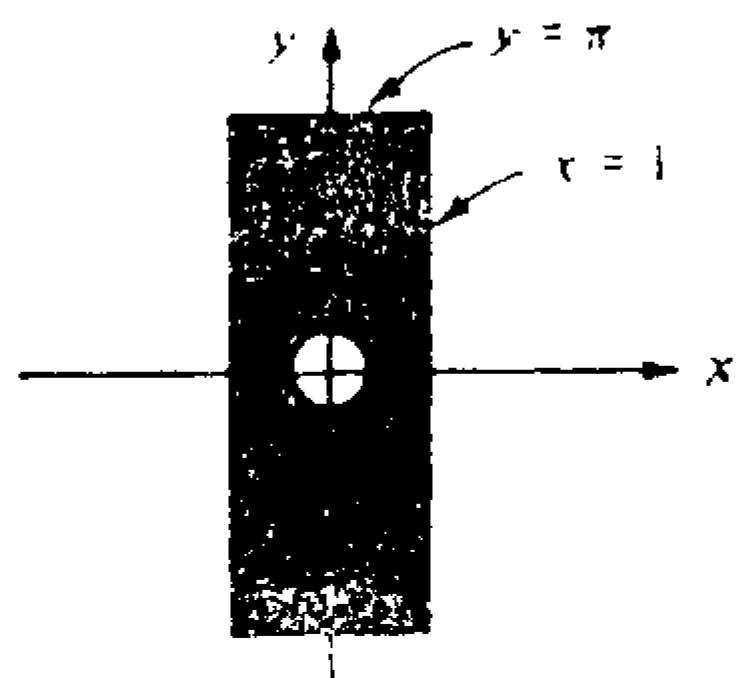
引理1 令$S(r)$表示一个区域，它是去掉z—平面的所

有半径为r的圆盘以后余下的部分．其中 $0<r<\pi$，圆心是 $z=2n\pi i$，$n=0$，±1，$\pm2\cdots$．如果$0<a\leqslant1$，则函数

$$g(z)=\frac{e^{az}}{1-e^z}$$

在$s(r)$里是有界的．（这个界依赖于r．）

证明　我们写$z=x+iy$，并考虑如图12.2所示的有孔的长方形



（图12.2）

$$Q(r)=\{z:|x|\leqslant1,\ |y|\leqslant\pi,\ |z|\geqslant r\}$$

这是一个紧集合，所以g在$Q(r)$上是有界的．还因为$|g(z+2\pi i)|=|g(z)|$，所以g在有孔的无穷带形区域

$$\{z:|x|\leqslant1,\ |z-2n\pi i|\geqslant r, n=0,\ \pm1,\ \pm2,\ \cdots\}$$

里也是有界的．

现在我们证明，g在这个带形的外面也是有界的．假设$|x|\geqslant1$并考虑

$$|g(z)|=\left|\frac{e^{az}}{1-e^z}\right|=\frac{e^{ax}}{|1-e^z|}\leqslant\frac{e^{ax}}{|1-e^x|}.$$

对$x\geqslant1$，我们有$|1-e^x|=e^x-1$与$e^{ax}\leqslant e^x$，所以

$$|g(z)|\leqslant\frac{e^x}{e^x-1}=\frac{1}{1-e^{-x}}\leqslant\frac{1}{1-e^{-1}}=\frac{e}{e-1}.$$

还有，当$x\leqslant-1$时，我们有$|1-e^x|=1-e^x$，所以

$$|g(z)|\leqslant\frac{e^{ax}}{1-e^x}\leqslant\frac{1}{1-e^x}\leqslant\frac{1}{1-e^{-1}}=\frac{e}{e-1}.$$

因此，对$|x|\geqslant1$有$|g(z)|\leqslant\dfrac{e}{(e-1)}$．引理证明完成．　□

现在我们回到Hurwitz公式．这包含由

$$(9)\quad F(x, s)=\sum_{n=1}^{\infty}\frac{e^{2\pi i n x}}{n^s}$$

给出的另一个Dirichlet 级数 $F(x, s)$，其中x是实数并且$\sigma>1$．注意$F(x, s)$是一个周期为1的周期函数并且$F(1, s)=\zeta(s)$，当$\sigma>1$时，这个级数绝对收敛。如果x不是一个整数，那么级数对$\sigma>0$也收敛（条件收敛），因为对每一个固定的非整数x，其系数的部分和是有界的。

注：以后我们把$F(x, s)$看作周期zeta函数．

定理12.6 Hurwitz公式．如果$0<a\leqslant1$，$\sigma>1$，则我们有

$$(10)\quad \zeta(1-s, a)=\frac{\Gamma(s)}{(2\pi)^s}\left\{e^{-\frac{\pi i s}{2}}F(a, s)+e^{\frac{\pi i s}{2}}F(-a, s)\right\}.$$

如果$a\neq1$，这个表示式对$\sigma>0$也是正确的．

证明　讨论函数

$$I_N(s, a)=\frac{1}{2\pi i}\int_{c(N)}\frac{z^{s-1}e^{az}}{1-e^z}dz,$$

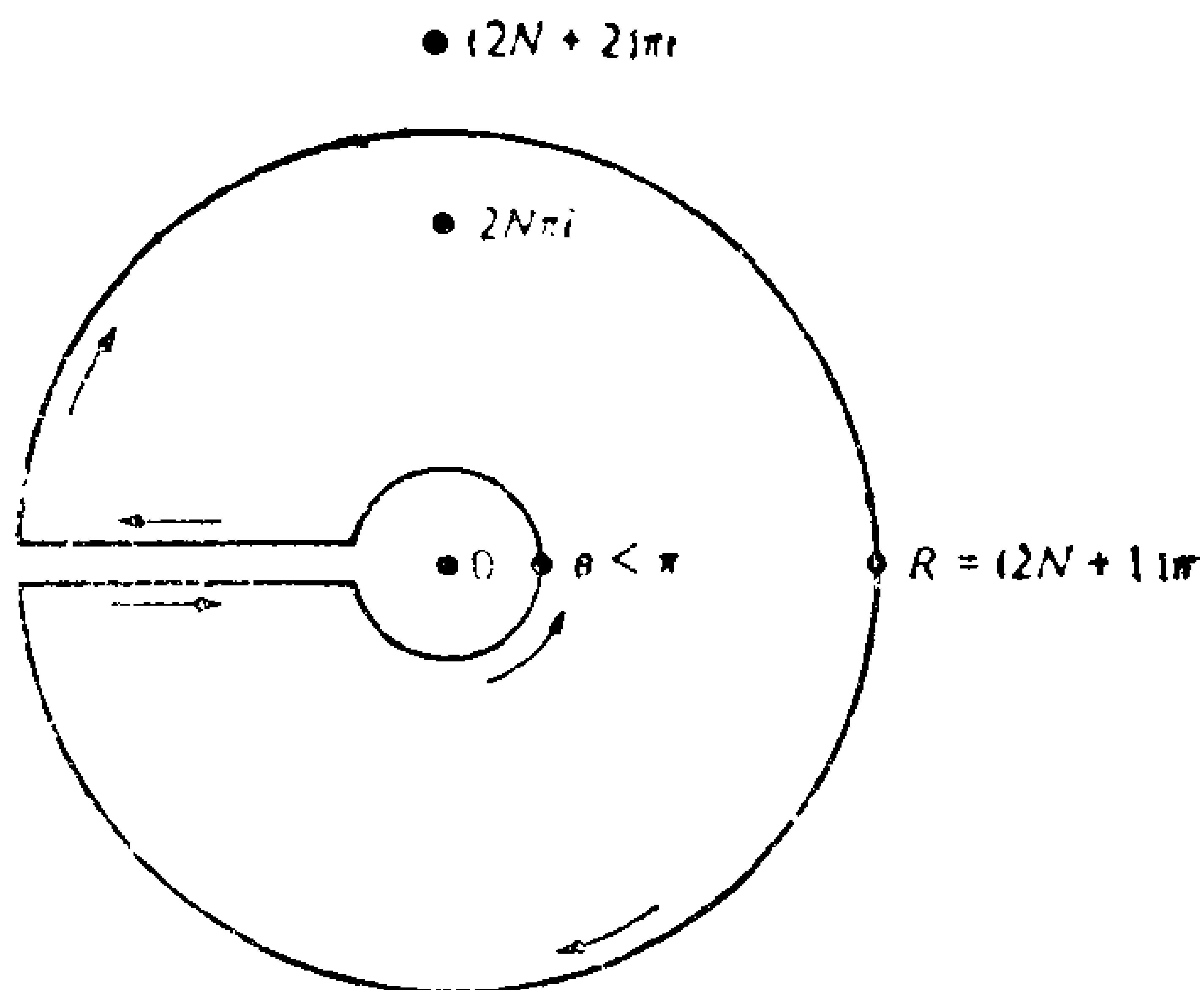
其中$c(N)$是图12.3所示的周界，N是一个整数．

首先我们证明，当$\sigma<0$时，$\lim_{N\to\infty}I_N(s, a)=I(s, a)$．为此，若能证明，当$N\to\infty$时，沿着圆周外部的积分趋于0就足够了．

在圆周外面我们有$z=Re^{i\theta}$，$-\pi\leqslant\theta\leqslant\pi$，于是

$$|z^{s-1}|=|R^{s-1}e^{i\theta(s-1)}|=R^{\sigma-1}e^{-t\theta}\leqslant R^{\sigma-1}e^{\pi|t|}.$$

因为圆的外部位于引理1中的集合$s(r)$里，被积函数不超过$Ae^{\pi|t|}R^{\sigma-1}$，其中A是由引理1推出的$|g(z)|$的界．于是



（图12.3）

积分不超过

$$2\pi A e^{\pi|t|}R^{\sigma},$$

若$\sigma<0$，当$R\to\infty$时，此式$\to0$. 因此，用$1-s$去代替s，我们得

(11) $\lim\limits_{N\to\infty}I_N(1-s,\ a)=I(1-s,\ a)$若$\sigma>1$.

现在我们计算$I_N(1-s,\ a)$，显然，根据Cauchy残数定理，我们有

$$I_N(1-s,a)=-\sum_{\substack{n=-N\\n\neq0}}^{N}R(n)$$

$$=-\sum_{n=1}^{N}\{R(n)+R(-n)\},$$

其中

$$R(n)=\operatorname*{Res}_{z=2n\pi i}\left(\frac{z^{-s}e^{az}}{1-e^{z}}\right).$$

于是

$$R(n)=\lim_{z\to2n\pi i}(z-2n\pi i)\frac{z^{-s}e^{az}}{1-e^{z}}$$

$$=\frac{e^{2n\pi i a}}{(2n\pi i)^s}\lim_{z\to 2n\pi i}\frac{z-2n\pi i}{1-e^z}$$
$$=-\frac{e^{2n\pi i a}}{(2n\pi i)^s},$$

$$I_N(1-s,\ a)=\sum_{n=1}^{N}\frac{e^{2n\pi i a}}{(2n\pi i)^s}+\sum_{n=1}^{N}\frac{e^{-2n\pi i a}}{(-2n\pi i)^s}.$$

但是$i^{-s}=e^{-\frac{\pi i s}{2}}$，$(-i)^{-s}=e^{\frac{\pi i s}{2}}$，所以

$$I_N(1-s,\ a)=\frac{e^{-\frac{\pi i s}{2}}}{(2\pi)^s}\sum_{n=1}^{N}\frac{e^{2n\pi i a}}{n^s}$$
$$+\frac{e^{\frac{\pi i s}{2}}}{(2\pi)^s}\sum_{n=1}^{N}\frac{e^{-2n\pi i a}}{n^s},$$

令$N\to\infty$并利用(11)我们得

$$I_N(1-s,\ a)=\frac{e^{-\frac{\pi i s}{2}}}{(2\pi)^s}F(a,\ s)$$
$$+\frac{e^{\frac{\pi i s}{2}}}{(2\pi)^s}F(-a,\ s).$$

于是

$$\zeta(1-s,\ a)=\Gamma(s)I(1-s,\ a)$$
$$=\frac{\Gamma(s)}{(2\pi)^s}\left\{e^{-\frac{\pi i s}{2}}F(a,\ s)+e^{\frac{\pi i s}{2}}F(-a,\ s)\right\}.$$

□

12.8 Riemann zeta函数的函数方程

Hurwitz公式的第一个应用ζ(s)的Riemann函数方程.

定理12.7 对所有的s，我们有

(12) $\zeta(1-s)=2(2\pi)^{-s}\Gamma(s)\cos\left(\frac{\pi s}{2}\right)\zeta(s)$,

或者，等价地，有

(13) $\zeta(s)=2(2\pi)^{s-1}\Gamma(1-s)\sin\left(\frac{\pi s}{2}\right)\zeta(1-s)$.

证明　在Hurwitz公式里取$a=1$，对$\sigma>1$，有

$$\zeta(1-s)=\frac{\Gamma(s)}{(2\pi)^s}\left\{e^{-\frac{\pi is}{2}}\zeta(s)+e^{\frac{\pi is}{2}}\zeta(s)\right\}$$

$$=\frac{\Gamma(s)}{(2\pi)^s}2\cos\left(\frac{\pi s}{2}\right)\zeta(s).$$

这证明(12)对$\sigma>1$成立，根据解析开拓，对所有s都成立。用$1-s$代替s，由(12)得出(13)。 □

注. 在(12)里取$s=2n+1$，其中$n=1, 2, 3, \cdots$，因子$\cos\left(\frac{\pi s}{2}\right)$为零，我们得到$\zeta(s)$的平凡零点，

$$\zeta(-2n)=0 \quad 对n=1, 2, 3, \cdots.$$

如果我们利用gamma函数的Legendre倍角公式，这个函数方程能写为一个简单的形式

$$2\pi^{\frac{1}{2}}2^{-2s}\Gamma(2s)=\Gamma(s)\Gamma\left(s+\frac{1}{2}\right),$$

它是方程(4)的特殊情形$m=2$. 当s被$\frac{(1-s)}{2}$代替时，它变为

$$2^s\pi^{\frac{1}{2}}\Gamma(1-s)=\Gamma\left(\frac{1-s}{2}\right)\Gamma\left(1-\frac{s}{2}\right).$$

因为

$$\Gamma\left(\frac{s}{2}\right)\Gamma\left(1-\frac{s}{2}\right)=\frac{\pi}{\sin\frac{\pi s}{2}},$$

这给出

$$\Gamma(1-s)\sin\frac{\pi s}{2}=\frac{2^{-s}\pi^{\frac{1}{2}}\Gamma\left(\frac{1-s}{2}\right)}{\Gamma\left(\frac{s}{2}\right)}.$$

利用此式去代替(13)里的乘积$\Gamma(1-s)\sin\left(\frac{\pi s}{2}\right)$，得

$$\pi^{\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\zeta(s)=\pi^{\frac{-(1-s)}{2}}\Gamma\left(\frac{1-s}{2}\right)\zeta(1-s).$$

换言之，函数方程取形式

$$\Phi(s)=\Phi(1-s),$$

其中

$$\Phi(s)=\pi^{\frac{-s}{2}}\Gamma\left(\frac{s}{2}\right)\zeta(s).$$

函数$\Phi(s)$有简单极点$s=0$与$s=1$，为了去掉极点，我们用$\frac{s(s-1)}{2}$去乘$\Phi(s)$并定义

$$\xi(s)=\frac{1}{2}s(s-1)\Phi(s),$$

则$\xi(s)$是s的一个整函数并满足方程

$$\xi(s)=\xi(1-s).$$

12.9 Hurwitz zeta函数的函数方程

$\zeta(s)$的函数方程是$\zeta(s, a)$的函数方程在a为有理数时的一个特殊情形.

定理12.8 如果h与k都是整数，$1\leqslant h\leqslant k$，那么对所有的s，我们有

(14) $$\zeta\left(1-s, \frac{h}{k}\right)=\frac{2\Gamma(s)}{(2\pi k)^{s}}\sum_{r=1}^{k}\cos\left(\frac{\pi s}{2}-\frac{2\pi rh}{k}\right)\zeta\left(s, \frac{r}{k}\right).$$

证明　此结果来自于这样一个事实，即当x是有理数时，函数F(x, s)是Hurwitz zeta函数的一个线性组合．实际上，如果 $x=\frac{h}{k}$，我们可根据模k的剩余类重排(8)里的项，写

$$n=qk+r，其中1\leqslant r\leqslant k，q=0, 1, 2, \cdots$$

这给出，对$\sigma>1$，

$$\begin{aligned}F\left(\frac{h}{k}, s\right)&=\sum_{n=1}^{\infty}\frac{e^{\frac{2\pi inh}{k}}}{n^{s}}\\&=\sum_{r=1}^{k}\sum_{q=0}^{\infty}\frac{e^{\frac{2\pi irh}{k}}}{(qk+r)^{s}}\\&=\frac{1}{k^{s}}\sum_{r=1}^{k}e^{\frac{2\pi irh}{k}}\sum_{q=0}^{\infty}\frac{1}{\left(q+\frac{r}{k}\right)^{s}}\\&=k^{-s}\sum_{r=1}^{k}e^{\frac{2\pi irh}{k}}\zeta\left(s, \frac{r}{k}\right).\end{aligned}$$

因此，如果我们在Hurwitz公式里取$a=\frac{h}{k}$，则有

$$\begin{aligned}\zeta\left(1-s, \frac{h}{k}\right)=\frac{\Gamma(s)}{(2\pi k)^{s}}\sum_{r=1}^{k}\Big(&e^{\frac{-\pi is}{2}}e^{\frac{2\pi irh}{k}}\\&+e^{\frac{\pi is}{2}}e^{\frac{-2\pi irh}{k}}\Big)\zeta\left(s, \frac{r}{k}\right)\end{aligned}$$

$$=\frac{2\Gamma(s)}{(2\pi k)^s}\sum_{r=1}^{k}\cos\left(\frac{\pi s}{2}-\frac{2\pi rh}{k}\right)\zeta\left(s,\ \frac{r}{k}\right),$$

这证明(14)对$\sigma>1$成立，根据解析开拓，此结果对所有的 s 成立. □

应当指出，当$h=k=1$时，(14)里的和仅有一项，并且我们得到Riemann函数方程.

12.10 L-函数的函数方程

Hurwitz公式也可用于推导DirichletL-函数的函数方程. 首先，我们指出，只讨论模k的本原特征就够了.

定理12.9 令χ是模k的任一Dirichlet特征，d是任一诱导模，并写

$$\chi(n)=\psi(n)\chi_1(n),$$

其中ψ是模d的特征，χ_1是模k的主特征，那么，对所有的s，我们有

$$L(s,\ \chi)=L(s,\ \psi)\prod_{p\mid k}\left(1-\frac{\psi(p)}{p^s}\right).$$

证明 首先，保持$\sigma>1$，并利用Euler乘积

$$L(s,\ \chi)=\prod_{p}\frac{1}{1-\frac{\chi(p)}{p^s}},$$

因为$\chi(p)=\psi(p)\chi_1(p)$，并且当$p\mid k$时，$\chi_1(p)=0$，当$p\nmid k$时，$\chi_1(p)=1$，我们得

$$L(s, x)=\prod_{p \nmid k} \frac{1}{1-\dfrac{\psi(p)}{p^{s}}}$$

$$=\prod_{p} \frac{1}{1-\dfrac{\psi(p)}{p^{s}}} \cdot \prod_{p \mid k}\left(1-\frac{\psi(p)}{p^{s}}\right)$$

$$=L(s, \psi) \prod_{p \mid k}\left(1-\frac{\psi(p)}{p^{s}}\right).$$

这证明定理对$\sigma>1$成立．根据解析开拓，我们可扩大它对所有的s成立． □

注：如果我们在上面的定理中假设d是x的前导子，那么ψ是d的本原特征，这说明每一个L一级数L（s，x）等于本原特征的L一级数L（s，χ）乘以有限个因子．

为了由Hurwitz公式推导出L-函数的函数方程，我们先用周期zeta函数$F(x, s)$来表示$L(s, \chi)$．

定理12.10　令χ是模K的一个本原特征，那么对$\sigma>1$，我们有

$$(15)\quad G(1, \bar{\chi}) L(s, \chi)=\sum_{h=1}^{k} \bar{\chi}(h) F\left(\frac{h}{k}, s\right),$$

其中$G(m, \chi)$是与χ相伴的Gauss和，

$$G(m, \chi)=\sum_{r=1}^{k} \chi(r) e^{\frac{2 \pi i r m}{k}}.$$

证明　在(9)里取$x=\dfrac{h}{k}$，用$\bar{\chi}(h)$乘之并对h求和，得

$$\sum_{h=1}^{k} \bar{\chi}(h) F\left(\frac{h}{k}, s\right)=\sum_{h=1}^{k} \sum_{n=1}^{\infty} \bar{\chi}(h) e^{\frac{2 \pi i n h}{k}} n^{-s}$$

$$=\sum_{n=1}^{\infty} n^{-s} \sum_{h=1}^{k} \bar{\chi}(h) e^{\frac{2 \pi i n h}{k}}$$

$$=\sum_{n=1}^{\infty} n^{-s}G(n,\overline{\chi}).$$

因$\overline{\chi}$是本原的，故$G(n,\overline{\chi})$是可分的，所以$G(n,\overline{\chi})=\chi(n)G(1,\overline{\chi})$，于是

$$\sum_{h=1}^{k}\overline{\chi}(h)F\left(\frac{h}{k},\ s\right)=G(1,\ \overline{\chi})\sum_{n=1}^{\infty}\chi(n)n^{-s}$$

$$=G(1,\ \overline{\chi})L(s,\ \chi).\qquad\square$$

定理12.11 Dirichlet L-函数的函数方程．如果χ是模K的任一本原特征，那么对所有的s，我们有

$$(16)\quad L(1-s,\ \chi)=\frac{k^{s-1}\Gamma(s)}{(2\pi)^s}\left\{e^{\frac{-\pi is}{2}}+\chi(-1)e^{\frac{\pi is}{2}}\right\}G(1,\ \chi)L(s,\ \overline{\chi}).$$

证明　在Hurwitz公式里取$x=\dfrac{h}{k}$，然后用$\chi(h)$乘每一部分并对h求和，得

$$\sum_{h=1}^{k}\chi(h)\zeta\left(1-s,\ \frac{h}{k}\right)$$

$$=\frac{\Gamma(s)}{(2\pi)^s}\left\{e^{\frac{-\pi is}{2}}\sum_{h=1}^{k}\chi(h)F\left(\frac{h}{k},\ s\right)+e^{\frac{\pi is}{2}}\sum_{h=1}^{k}\chi(h)F\left(-\frac{h}{k},\ s\right)\right\}.$$

因为$F(x,\ s)$是周期为1的对x的周期函数，并且$\chi(h)=\chi(-1)\chi(-h)$，我们可写

$$\sum_{h\bmod k}\chi(h)F\left(-\frac{h}{k},\ s\right)$$

$$=\chi(-1)\sum_{h\bmod k}\chi(-h)F\left(-\frac{h}{k},\ s\right)$$

$$=\chi(-1)\sum_{h \bmod k}\chi(k-h)F\left(\frac{k-h}{k}, s\right)$$

$$=\chi(-1)\sum_{h \bmod k}\chi(h)F\left(\frac{h}{k}, s\right),$$

于是，前面的式子变为

$$\sum_{h=1}^{k}\chi(h)\zeta\left(1-s, \frac{h}{k}\right)$$

$$=\frac{\Gamma(s)}{(2\pi)^s}\left\{e^{-\frac{\pi i s}{2}}+\chi(-1)e^{\frac{\pi i s}{2}}\right\}$$

$$\sum_{h=1}^{k}\chi(h)F\left(\frac{h}{k}, s\right).$$

用k^{s-1}去乘两边并利用(15)即得(16). □

12.11 求$\zeta(-n, a)$的值

当n是一个非负整数时，$\zeta(-n, a)$的值能直接算出．在关系式$\zeta(s, a)=\Gamma(1-s)I(s, a)$中取$s=-n$，得

$$\zeta(-n, a)=\Gamma(1+n)I(-n, a)=n!I(-n, a).$$

我们还有

$$I(-n, a)=\operatorname*{Res}_{z=0}\left(\frac{z^{-n-1}e^{az}}{1-e^z}\right),$$

由这个残数的计算引出一个有趣的称为 Bernoulli 多项式的函数类.

定义 对任一复数x，由方程

$$\frac{ze^{xz}}{e^z-1}=\sum_{n=0}^{\infty}\frac{B_n(x)}{n!}z^n \quad 其中|z|\leqslant 2\pi$$

定义函数$B_n(x)$．数$B_n(0)$称为Bernoulli数并记为B_n，即

$$\frac{z}{e^z-1}=\sum_{n=0}^{\infty}\frac{B_n}{n!}z^n,\text{ 其中}|z|\leqslant 2\pi.$$

定理12.12　函数$B_n(x)$是由

$$B_n(x)=\sum_{k=0}^{n}\binom{n}{k}B_k x^{n-k}$$

给定的x的多项式.

证明　我们有

$$\sum_{n=0}^{\infty}\frac{B_n(x)}{n!}z^n=\frac{z}{e^z-1}e^{xz}$$

$$=\left(\sum_{n=0}^{\infty}\frac{B_n}{n!}z^n\right)\left(\sum_{n=0}^{\infty}\frac{x^n}{n!}z^n\right).$$

由于z^n的系数相等，我们得

$$\frac{B_n(x)}{n!}=\sum_{k=0}^{n}\frac{B_k}{k!}\frac{x^{n-k}}{(n-k)!}.$$

由此即得定理. □

定理12.13　对每一个整数$n\geqslant 0$，我们有

$$(17)\quad \zeta(-n,a)=\frac{-B_{n+1}(a)}{n+1}.$$

证明　如前所述，我们有 $\zeta(-n,a)=n!I(-n,a)$，而

$$I(-n,a)=\operatorname*{Res}_{z=0}\left(\frac{z^{-n-1}e^{az}}{1-e^z}\right)$$

$$=-\operatorname*{Res}_{z=0}\left(z^{-n-2}\frac{ze^{az}}{e^z-1}\right)$$

$$=-\operatorname*{Ret}_{z=0}\left(z^{-n-2}\sum_{m=0}^{\infty}\frac{B_m(a)}{m!}z^m\right)$$

$$=-\frac{B_{n+1}(a)}{(n+1)!}.$$

由此得(17). □

12.12 Bernoulli数与Bernoulli多项式的性质

定理12.14 **Bernoulli多项式$B_n(x)$满足差分方程**

(18) $B_n(x+1)-B_n(x)=nx^{n-1}$ **若$n\geqslant 1$.**

因此有

(19) $B_n(0)=B_n(1)$ **若** $n\geqslant 2$.

证明 我们有等式

$$z\frac{e^{(x+1)z}}{e^z-1}-z\frac{e^{xz}}{e^z-1}=ze^{xz}.$$

由此得

$$\sum_{n=0}^{\infty}\frac{B_n(x+1)-B_n(x)}{n!}z^n=\sum_{n=0}^{\infty}\frac{x^n}{n!}z^{n+1}.$$

由z^n的系数相等我们得(18). 在(18)里取$x=0$得(19). □

定理12.15 **当$n\geqslant 2$时，我们有**

$$B_n=\sum_{k=0}^{n}\binom{n}{k}B_k.$$

证明 在定理12.12里取$x=1$并利用(19)即得. □

定理12.15给出一个计算Bernoulli数的递推公式. 定义已给定$B_0=1$，由定理12.15可接连地得出一些值，

$$B_0=1,\quad B_1=-\frac{1}{2},\quad B_2=\frac{1}{6},\quad B_3=0,$$

$$B_4=-\frac{1}{30},\quad B_5=0,\quad B_6=\frac{1}{42},\quad B_7=0,$$

$$B_8=-\frac{1}{30},\quad B_9=0,\quad B_{10}=\frac{5}{66},\quad B_{11}=0.$$

由一个已知的B_k，利用定理12.12能算出多项式$B_n(x)$，前面几个是

$$B_0(x)=1,\quad B_1(x)=x-\frac{1}{2},\quad B_2(x)=x^2-x+\frac{1}{6},$$

$$B_3(x)=x^3-\frac{3}{2}x^2+\frac{1}{2}x,$$

$$B_4(x)=x^4-2x^3+x^2-\frac{1}{30}.$$

根据定理12.12与定理12.15，可写如下符号：

$$B_n(x)=(B+x)^n,\quad B_n=(B+1)^n.$$

在这两个式子里，右边部分按二项式定理展开，然后把每一个方幂B^k用B_k代替.

定理12.16　如果$n\geqslant 0$，则有

$$(20)\qquad \zeta(-n)=-\frac{B_{n+1}}{n+1},$$

此外，当$n\geqslant 1$时，我们有$\zeta(-2n)=0$，$B_{2n+1}=0$.

证明　为计算$\zeta(-n)$的值，我们在定理12.13里取 $a=1$ 即得(20).

我们已经指出过，函数方程

$$(21)\qquad \zeta(1-s)=2(2\pi)^{-s}\Gamma(s)\cos\left(\frac{\pi s}{2}\right)\zeta(s).$$

推出$\zeta(-2n)=0$对$n\geqslant 1$. 于是根据(20)得$B_{2n+1}=0$. □

注：$B_{2n+1}=0$这一结果也可由

$$\frac{z}{e^z-1}+\frac{1}{2}z=1+\sum_{n=2}^{\infty}\frac{B_n}{n!}z^n$$

的左边是z的一个偶函数而得到.

定理12.17　如果K是一个正整数，则有

$$(22)\qquad \zeta(2K)=(-1)^{k+1}\frac{(2\pi)^{2k}B_{2k}}{2(2K)!}.$$

证明　在$\zeta(s)$的函数方程里取$s=2k$，得

$$\zeta(1-2k)=2(2\pi)^{-2k}\Gamma(2k)\cos(\pi k)\zeta(2k),$$

或者

$$-\frac{B_{2k}}{2k}=2(2\pi)^{-2k}(2k-1)!(-1)^k\zeta(2k).$$

这就推出(22). □

注意，如果我们在(21)里令$s=2k+1$，则(21)两端为0，因而我们不能得到关于$\zeta(2k+1)$的情况.迄今，对$\zeta(2k+1)$没有得到类似于(22)的公式，甚至对任一特殊情形，例如$\zeta(3)$也不知道.对任意的整数k，$\zeta(2k+1)$是有理数或无理数都不知道.

定理12.18 Bernoulli数B_{2k}交替变号，即

$$(-1)^{k+1}B_{2k}>0.$$

此外还有，当$K\to\infty$时，$|B_{2k}|\to\infty$. 实际上

$$(23)\quad (-1)^{k+1}B_{2k}\sim\frac{2(2K)!}{(2\pi)^{2k}}\quad 当K\to\infty时.$$

证明 因为$\zeta(2k)>0$，(22)就说明B_{2k}交替变号.当$k\to\infty$时，$\zeta(2k)\to1$，因此得(23). □

注意，当$k\to\infty$时，由(23)立即得出$\left|\frac{B_{2k+2}}{B_{2k}}\right|\sim\frac{k^2}{\pi^2}$. 并根据 Stirling 公式$n!\sim\left(\frac{n}{e}\right)^n\sqrt{2\pi n}$，得

$$(-1)^{k+1}B_{2k}\sim4\pi\sqrt{e}\left(\frac{k}{\pi e}\right)^{\frac{2k+1}{2}}\quad 当k\to\infty时.$$

下一个定理给出多项式$B_n(x)$在区间$0<x\leqslant1$里的Fourier展式.

定理12.19 如果$0<x\leqslant1$，则有

$$(24)\quad B_n(x)=-\frac{n!}{(2\pi i)^n}\sum_{\substack{k=-\infty\\k\neq0}}^{+\infty}\frac{e^{2\pi ikx}}{K^n},$$

于是有

$$B_{2n}(x)=(-1)^{n+1}\frac{2(2n)!}{(2\pi)^{2n}}\sum_{k=1}^{\infty}\frac{\cos 2\pi kx}{k^{2n}},$$

$$B_{2n+1}(x)=(-1)^{n+1}\frac{2(2n+1)!}{(2\pi)^{2n+1}}\sum_{k=1}^{\infty}\frac{\sin 2\pi kx}{k^{2n+1}}.$$

证明　在Hurwitz公式里取$s=n$并应用定理12.13立即得(24)．另两个式子是(24)的特殊情形．□

注：(24)右端对所有实数定义的函数$\overline{B}_n(x)$叫做n次Bernoulli周期函数，其周期为1．在区间$0<x\leqslant 1$里，它与Bernoulli多项式$B_n(x)$相同，即

$$\overline{B}_n(x)=B_n(x-[x]).$$

12.13　$L(0,\ \chi)$的公式

定理12.13推出

$$\zeta(0,\ a)=-B_1(a)=\frac{1}{2}-a.$$

特别，$\zeta(0)=\zeta(0,\ 1)=-\frac{1}{2}$．对每一个 Dirichlet特征$\chi$，我们还能算出$L(0,\ \chi)$．

定理12.20　令χ是模K的任一Dirichlet特征，

(a)　如果$\chi=\chi_1$（即主特征），则$L(0,\ \chi_1)=0$．

(b)　如果$\chi\neq\chi_1$，则有

$$L(0,\ \chi)=-\frac{1}{K}\sum_{r=1}^{k}r\chi(r).$$

还有，如果$\chi(-1)=1$，则$L(0,\ \chi)=0$．

证明　当$\chi=\chi_1$时，我们利用在第十一章里证明过的对$\sigma>1$成立的公式

$$L(s,\ \chi_1)=\zeta(s)\prod_{p\mid k}(1-p^{-s}).$$

根据解析开拓，这个公式对所有的s也成立.
当$s=0$时，式中乘积为0，所以$L(0, \chi_1)=0$.

如果$\chi=\chi_1$，我们有

$$L(0, \chi)=\sum_{r=1}^{k}\chi(r)\zeta\left(0, \frac{r}{k}\right)$$
$$=\sum_{r=1}^{k}\chi(r)\left(\frac{1}{2}-\frac{r}{k}\right)$$
$$=-\frac{1}{k}\sum_{r=1}^{k}r\chi(r),$$

于是

$$\sum_{r=1}^{k}r\chi(r)=\sum_{r=1}^{k}(k-r)\chi(k-r)$$
$$=k\sum_{r=1}^{k}\chi(k-r)-\sum_{r=1}^{k}r\chi(-r)$$
$$=-\chi(-1)\sum_{r=1}^{k}r\chi(r).$$

因此，当$\chi(-1)=1$时，我们有$\sum_{r=1}^{k}r\chi(r)=0$. □

12.14 用有限和逼近$\zeta(s, a)$

一些应用需要计算作为t的函数$\zeta(\sigma+it, a)$的增长率，这将由Euler求和公式得到$\zeta(s, a)$的另一个表示式来算出.在半平面$\sigma>0$里，$\zeta(s, a)$与它的级数的部分和有关并且还给出在直线$\sigma=1$之外展开$\zeta(s, a)$的解析性的一个替代方法.

定理12.21　对任意整数$N\geqslant 0$与$\sigma>0$，我们有

$$\zeta(s, a)=\sum_{n=0}^{N}\frac{1}{(n+a)^s}+\frac{(N+a)^{1-s}}{s-1} \tag{25}$$

$$-s\int_N^{\infty}\frac{x-[x]}{(x+a)^{s+1}}dx.$$

证明　我们应用 Euler 求和公式(定理3.1)，因为 $f(t)=(t+a)^{-s}$ 且 x 与 y 都是整数，得

$$\sum_{y<n\leqslant x}\frac{1}{(n+a)^s}=\int_y^x\frac{dt}{(t+a)^s}-s\int_y^x\frac{t-[t]}{(t+a)^{s+1}}dt,$$

取 $y=N$ 并令 $x\to\infty$，保持 $\sigma>1$，得出

$$\sum_{n=N+1}^{\infty}\frac{1}{(n+a)^s}=\int_N^{\infty}\frac{dt}{(t+a)^s}-s\int_N^{\infty}\frac{t-[t]}{(t+a)^{s+1}}dt,$$

或

$$\zeta(s,\ a)-\sum_{n=0}^{N}\frac{1}{(n+a)^s}=\frac{(N+a)^{1-s}}{s-1}-s\int_N^{\infty}\frac{t-[t]}{(t+a)^{s+1}}dt.$$

这证明了(25)对 $\sigma>1$ 成立．如果 $\sigma\geqslant\delta>0$，其中积分不超过 $\int_N^{\infty}(t+a)^{-\delta-1}dt$，所以它对 $\sigma\geqslant\delta$ 一致收敛．于是，在半平面 $\delta>0$ 里，它表示一个解析函数，因此，根据解析开拓，(25)对 $\sigma>0$ 成立． □

(25)右端的积分还能写为级数，我们把这个积分写为一些积分的和，其中 $[x]$ 是常数，$[x]=n$，我们得

$$\int_N^{\infty}\frac{x-[x]}{(x+a)^{s+1}}dx=\sum_{n=N}^{\infty}\int_n^{n+1}\frac{x-n}{(x+a)^{s+1}}dx=\sum_{n=N}^{\infty}\int_0^1\frac{u}{(u+n+a)^{s+1}}du.$$

因此，(25)也可写为

$$(26)\quad \zeta(s,\ a)-\sum_{n=0}^{N}\frac{1}{(n+a)^{s}}$$

$$=\frac{(N+a)^{1-s}}{s-1}-s\sum_{n=N}^{\infty}\int_{0}^{1}\frac{u}{(u+n+a)^{s+1}}du.$$

当$\sigma>0$时．在逐步扩大的半平面里用分部积分法可推出类似的表示，如下面定理所指出的那样．

定理12.22　如果$\sigma>-1$，则有

$$(27)\quad \zeta(s,\ a)-\sum_{n=0}^{N}\frac{1}{(n+s)^{s}}$$

$$=\frac{(N+a)^{1-s}}{s-1}-\frac{s}{2!}\left\{\zeta(s+1,\ a)-\sum_{n=0}^{N}\frac{1}{(n+a)^{s+1}}\right\}$$

$$-\frac{s(s+1)}{2!}\sum_{n=N}^{\infty}\int_{0}^{1}\frac{u^{2}}{(n+a+u)^{s+2}}du,$$

更一般，如果$\sigma>-m$，$m=1,\ 2,\ 3,\ \cdots$，我们有

$$(28)\quad \zeta(s,\ a)-\sum_{n=0}^{N}\frac{1}{(n+a)^{s}}$$

$$=\frac{(N+a)^{1-s}}{s-1}-\sum_{r=1}^{m}\frac{s(s+1)\cdots(s+r-1)}{(r+1)!}$$

$$\times\left\{\zeta(s+r,\ a)-\sum_{n=0}^{N}\frac{1}{(n+a)^{s+r}}\right\}$$

$$-\frac{s(s+1)\cdots(s+m)}{(m+1)!}$$

$$\times\sum_{n=N}^{\infty}\int_{0}^{1}\frac{u^{m+1}}{(n+a+u)^{s+m+1}}du.$$

证明　由分部积分法得出

$$\int\frac{u\,du}{(n+a+u)^{s+1}}$$

$$= \frac{u^2}{2(n+a+u)^{s+1}} + \frac{s+1}{2}\int \frac{u^2 du}{(n+a+u)^{s+2}},$$

所以，如果$\sigma>0$，我们有

$$\sum_{n=N}^{\infty}\int_0^1 \frac{u du}{(n+a+u)^{s+1}}$$

$$= \frac{1}{2}\sum_{n=N}^{\infty}\frac{1}{(n+a+1)^{s+1}}$$

$$+ \frac{s+1}{2}\sum_{n=N}^{\infty}\int_0^1 \frac{u^2 du}{(n+a+u)^{s+2}}.$$

当$\sigma>0$时，右边的第一个和式是$\zeta(s+1, a)-\sum_{n=0}^{N}(n+a)^{-s-1}$并且(26)推出(27).根据解析开拓，此结果对$\sigma>-1$也是正确的，多次用分部积分法即得(28)里的更一般的表示式.

12.15 $|\zeta(s, a)|$的不等式

上一节的公式可得出t的函数$|\zeta(\sigma+it, a)|$的上界.

定理12.23 (a) 如果$\delta>0$，则有

(29) $|\zeta(s, a)-a^{-s}|\leqslant\zeta(1+\delta)$ 若$\sigma\geqslant 1+\delta$.

(b) 如果$0<\delta<1$，则有一个正的常数$A(\delta)$，它依赖于δ但不依赖于s或a，使得

(30) $|\zeta(s, a)-a^{-s}|\leqslant A(\delta)|t|^{\delta}$

若$1-\delta\leqslant\sigma\leqslant 2$, $|t|\geqslant 1$.

(31) $|\zeta(s, a)-a^{-s}|\leqslant A(\delta)|t|^{1+\delta}$

若$-\delta\leqslant\sigma\leqslant\zeta$, $|t|\geqslant 1$.

(32) $|\zeta(s, a)\leqslant A(\delta)|t|^{m+1+\delta}$

若$-m-\delta\leqslant\sigma\leqslant-m+\delta$, $|t|\geqslant 1$.

其中$m=1, 2, 3\cdots$.

证明 对于(a)，我们利用$\zeta(s, a)$所确定的级数，得

$$|\zeta(s, a)-a^{-s}|\leqslant\sum_{n=1}^{\infty}\frac{1}{(n+a)^{\sigma}}$$

$$\leqslant\sum_{n=1}^{\infty}\frac{1}{n^{1+\delta}}=\zeta(1+\delta),$$

这就是(29)式.

对于(b)，我们利用(25)里的表示式，当$1-\delta\leqslant\sigma\leqslant2$时，得

$$|\zeta(s, a)-a^{-s}|\leqslant\sum_{n=1}^{N}\frac{1}{(n+a)^{\sigma}}+\frac{(N+a)^{1-\sigma}}{|s-1|}$$

$$+|s|\int_{N}^{\infty}\frac{dx}{(x+a)^{\sigma+1}}$$

$$<1+\int_{1}^{N}\frac{dx}{(x+a)^{\sigma}}+\frac{(N+a)^{1-\sigma}}{|s-1|}$$

$$+\frac{|s|}{\sigma}(N+a)^{-\sigma}.$$

因为$\sigma\geqslant1-\delta>0$，我们有$(x+a)^{\sigma}\geqslant(x+a)^{1-\delta}>x^{1-\delta}$，所以，

$$\int_{1}^{N}\frac{dx}{(x+a)^{\sigma}}\leqslant\int_{1}^{N}\frac{dx}{x^{1-\delta}}<\frac{N^{\delta}}{\delta}.$$

还因为$|s-1|=|\sigma-1+it|\geqslant|t|\geqslant1$，我们有

$$\frac{(N+a)^{1-\sigma}}{|s-1|}\leqslant(N+a)^{\delta}\leqslant(N+1)^{\delta}.$$

最后，因为$|s|\leqslant|\sigma|+|t|\leqslant2+|t|$，我们得

$$\frac{|s|}{\sigma}(N+a)^{-\delta}<\frac{2+|t|}{1-\delta}(N+a)^{\delta-1}$$

$$<\frac{2+|t|}{1-\delta}\frac{1}{N^{1-\delta}}.$$

这给我们

$$|\zeta(s, a)-a^{-s}|$$
$$<1+\frac{N^{\delta}}{\delta}+(N+1)^{\delta}+\frac{2+|t|}{1-\delta}\,\frac{N^{\delta}}{N}.$$

现在取$N=1+[|t|]$，那么最后三项是$O(|t|^{\delta})$，其中大O符号仅依赖于δ而得出常数$A(\delta)$，这证明了(30)．

为证明(31)，我们利用(27)里的表示式，得

$$\begin{aligned}|\zeta(s, a)-a^{-s}|\leqslant \sum_{n=1}^{N}\frac{1}{(n+a)^{\delta}}+\frac{(N+a)^{1-\sigma}}{|s-1|}\\
+\frac{1}{2}|s|\{|\zeta(s+1, a)-a^{-s-1}|\}\\
+\frac{1}{2}|s|\sum_{n=1}^{N}\frac{1}{(n+a)^{\sigma+1}}\\
+\frac{1}{2}|s||s+1|\sum_{n=N}^{\infty}\frac{1}{(n+a)^{\sigma+2}}.\end{aligned}$$

同(30)的证明一样，我们取$N=1+[|t|]$，所以$N=O(|t|)$，并且我们证明右端的每一项是$O(|t|^{1+\delta})$，其中常数由仅依赖于δ的大O符号推出．不等式$-\delta\leqslant\sigma\leqslant\delta$即$1-\delta\leqslant1+\sigma\leqslant1+\delta$，于是

$$\begin{aligned}\sum_{n=1}^{N}\frac{1}{(n+a)^{\sigma}}<1+\int_{1}^{N}\frac{dx}{(n+a)^{\sigma}}<1+\frac{(N+a)^{1-\sigma}}{1-\sigma}\\
\leqslant1+\frac{(N+1)^{1+\delta}}{1-\delta}=O(|t|^{1+\delta}).\end{aligned}$$

又因为$|s-1|\geqslant|t|\geqslant1$，所以第二项也是$O(|t|^{1+\delta})$．对于第三项．我们利用(30)，注意$1-\delta\leqslant\sigma+1\leqslant1+\delta$与
$|s|=O(|t|)$，我们看出，这一项也是$O(|t|^{1+\delta})$．下面，我们有

$$|s|\sum_{n=1}^{N}\frac{1}{(n+a)^{\sigma+1}}=O\left(|t|\int_1^N\frac{dx}{(x+a)^{1-\delta}}\right)$$
$$=O(|t|N^{-\delta})=O(|t|^{1-\delta})$$
$$=O(|t|^{1+\delta}).$$

最后，

$$|s||s+1|\sum_{n=N}^{\infty}\frac{1}{(n+a)^{\sigma+2}}$$
$$=O\left(|t|^2\int_N^{\infty}\frac{dx}{(x+a)^{\delta+2}}\right)=O(|t|^2N^{-\sigma-1})$$
$$=O(|t|^2N^{\delta-1})=O(|t|^{1+\delta}).$$

这完全证明了(31).

(32)的证明是类似的，我们还要利用(28)并注意到$a^{-\sigma}=O(1)$当$\sigma<0$时. □

12.16 $|\zeta(s)|$与$|L(s,\chi)|$的不等式

当$a=1$时，定理12.23里的估计式给出$|\zeta(s)|$的相应的估计式，它也引导出Dirichlet L一级数的上界. 如果$\sigma\geqslant1+\delta$，$\delta>0$，则$|\zeta(s)|$与$|L(s,\chi)|$二者均不超过$\zeta(1+\delta)$，所以，我们只讨论$\sigma\leqslant1+\delta$.

定理12.24 **令χ是模k的任一Dirichlet特征，并设$0<\delta<1$，那么，存在一个正的常数$A(\delta)$，它依赖于δ但与k或s无关，使得，对$s=\sigma+it$，$|t|\geqslant1$，有**

(33) $|L(s,\chi)|\leqslant A(\delta)|kt|^{m+1+\delta}$

当$-m-\delta\leqslant\sigma\leqslant-m+\delta$时，

其中$m=-1,0,1,2,\cdots$.

证明　我们回忆到关系式

$$L(s,\ \chi)=k^{-s}\sum_{r=1}^{k-1}\chi(r)\zeta\left(s,\ \frac{r}{k}\right).$$

当$m=1$，2，3，…时，我们利用(32)，得

$$|L(s,\ \chi)|\leqslant k^{-\sigma}\sum_{r=1}^{k-1}\left|\zeta\left(s,\ \frac{r}{k}\right)\right|$$

$$<k^{m+\delta}kA(\delta)|t|^{m+1+\delta},$$

这证明(33)对$m\geqslant 1$成立．如果$m=0$或-1，我们有

$$(34)\quad L(s,\ \chi)=\sum_{r=1}^{k-1}\frac{\chi(r)}{r^{s}}$$

$$+k^{-s}\sum_{r=1}^{k-1}\chi(r)\left\{\zeta\left(s,\ \frac{r}{k}\right)-\left(\frac{r}{k}\right)^{-s}\right\}.$$

因为$-m-\delta\leqslant\sigma\leqslant -m+\delta$，我们利用(30)与(31)，得

$$k^{-\sigma}\left|\zeta\left(s,\ \frac{r}{k}\right)-\left(\frac{r}{k}\right)^{-s}\right|\leqslant k^{m+\delta}A(\delta)|t|^{m+1+\delta},$$

所以(34)里的第二个和不超过$A(\delta)|kt|^{m+1+\delta}$，而第一个和式不超过

$$\sum_{r=1}^{k-1}\frac{1}{r^{\sigma}}\leqslant\sum_{r=1}^{k-1}r^{m+\delta}<1+\int_{1}^{k}x^{m+\delta}dx$$

$$=\frac{k^{m+1+\delta}}{m+1+\delta}\leqslant\frac{k^{m+1+\delta}}{\delta},$$

这个和也能并入估计数$A(\delta)|kt|^{m+1+\delta}$之内． □

第十二章习题

1． 令$f(n)$是一个模k的周期数论函数．

(a) 证明Dirichlet级数$\sum f(n)n^{-s}$对$\sigma>1$绝对收敛，并且当$\sigma>1$时，有

$$\sum_{n=1}^{\infty}\frac{f(n)}{n^s}=k^{-s}\sum_{r=1}^{k}f(r)\zeta\left(s,\frac{r}{k}\right).$$

(b) 如果 $\sum_{r=1}^{k}f(r)=0$，证明Dirichlet级数$\sum f(n)n^{-s}$对$\sigma>0$收敛，并且存在一个整函数$F(s)$，使得$\sigma>0$，有$F(s)=\sum f(n)n^{-s}$.

2. 如果x是实数并且$\sigma>1$，令$F(x, s)$表示周期zeta函数

$$F(x, s)=\sum_{n=1}^{\infty}\frac{e^{2\pi inx}}{n^s},$$

如果$0<a<1$，证明，由Furwitz公式可推出

$$F(a, s)=\frac{\Gamma(1-s)}{(2\pi)^{1-s}}\left\{e^{\frac{\pi i(1-s)}{2}}\zeta(1-s, a)+e^{\frac{\pi i(s-1)}{2}}\zeta(1-s, 1-a)\right\}.$$

3. 利用2题中的公式把$F(a, s)$的定义扩大到整个s一平面上. 如果$0<a<1$，证明扩大了的$F(a, s)$是s的一个整函数.

4. 如果$0<a<1$，$0<b<1$，令

$$\Phi(a, b, s)=\frac{\Gamma(s)}{(2\pi)^s}\{\zeta(s, a)F(b, 1+s)+\zeta(s, 1-a)F(1-b, 1+s)\},$$

其中F是2题中的函数. 证明

$$\frac{\Phi(a, b, s)}{\Gamma(s)\Gamma(-s)}=e^{\frac{\pi is}{2}}\{\zeta(s, a)\zeta(-s, 1-b)+\zeta(s, 1-a)\zeta(-s, b)\}+e^{-\frac{\pi is}{2}}\{\zeta(-s, 1-b)\zeta(s, 1-a)+\zeta(-s, b)\zeta(s, a)\}.$$

并推导出$\Phi(a, b, s)=\Phi(1-b, a, -s)$. 这个函数方程在椭圆模函数理论里是有用的.

在5，6，7题里，$\xi(s)$表示12.8节里介绍过的整函数

$$\xi(s)=\frac{1}{2}s(s-1)\pi^{\frac{-s}{2}}\Gamma\left(\frac{s}{2}\right)\zeta(s).$$

5. 证明，在直线$t=0$与$\sigma=\frac{1}{2}$上，$\xi(s)$是实的并且$\xi(0)=\xi(1)=\frac{1}{2}$

6. 证明，$\xi(s)$的零点（如果存在的话）全部位于区间$0\leqslant\sigma\leqslant1$内，并且它们的位置是关于$t=0$与$\sigma=\frac{1}{2}$对称的.

7. 证明，在临界区间$0<\sigma<1$内，$\zeta(s)$的零点与$\xi(s)$的零点位置相同，重数相同.

8. 令χ是模k的一个本原特征，定义

$$a=a(\chi)=\begin{cases}0 & \chi(-1)=1,\\ 1 & \chi(-1)=-1.\end{cases}$$

(a) 证明$L(s, \chi)$的函数方程有形式

$$L(1-s, \overline{\chi})$$
$$=\varepsilon(\chi)2(2\pi)^{-s}k^{s-\frac{1}{2}}\cos\left(\frac{\pi(s-a)}{2}\right)\Gamma(s)L(s, \chi),$$

其中$|\varepsilon(\chi)|=1$.

(b) 令

$$\xi(s, \chi)=\left(\frac{k}{\pi}\right)^{\frac{(s+a)}{2}}\Gamma\left(\frac{s+a}{2}\right)L(s, \chi),$$

证明，$\xi(1-s, \overline{\chi})=\varepsilon(\chi)\xi(s, \chi)$.

9. 参看第8题

(a) 证明$\xi(s,\chi)\neq 0$，当$\sigma>1$或$\sigma<0$时.

(b) 描述半平面$\sigma<0$里$L(s,\chi)$的零点的位置.

10. 令χ是模k的一个非本原特征，试描述$L(s,\chi)$在半平面$\sigma<0$里的零点位置.

11. 证明，Bernoulli多项式满足关系式

$$B_n(1-x)=(-1)^n B_n(x),\quad B_{2n+1}\left(\frac{1}{2}\right)=0$$

对每个$n\geqslant 0$.

12. 令B_n表示n次Bernoulli数，注意

$$B_2=\frac{1}{6}=1-\frac{1}{2}-\frac{1}{3},$$

$$B_4=-\frac{1}{30}=1-\frac{1}{2}-\frac{1}{3}-\frac{1}{5}$$

$$B_6=\frac{1}{42}=1-\frac{1}{2}-\frac{1}{3}-\frac{1}{7}.$$

这些式子说明了一个定理，该定理在1840年分别地被Von Staudt与Clausen发现：如果$n\geqslant 1$，我们有

$$B_{2n}=I_n-\sum_{p-1\mid 2n}\frac{1}{p},$$

其中I_n是一个整数而和式是对所有使$p-1$整除2n的素数p求和. 本题概括出一个应归于Lucas的证明.

(a) 证明

$$B_n=\sum_{k=0}^{n}\frac{1}{k+1}\sum_{r=0}^{k}(-1)^r\binom{k}{r}r^n.$$

[提示：写$x=\log\{1+(e^x-1)\}$并利用$\frac{x}{(e^x-1)}$的幂级数.]

(b) 证明

$$B_n=\sum_{k=0}^{n}\frac{k!}{k+1}c(n,\ k),$$

其中$c(n,\ k)$是一个整数.

(c) 如果a，b都是整数，并且$a\geqslant 2$，$b\geqslant 2$，$ab>4$，证明$ab|(ab-1)!$，这说明，在(b)的和式里，$k>3$，$k+1$是复合数，每一项都是整数.

(d) 如果p是素数，证明

$$\sum_{r=0}^{p-1}(-1)^r\binom{p-1}{r}r^n$$

$$\equiv\begin{cases}-1 & (\mathrm{mod}\,p) \quad 若 p-1|n,\ n>0, \\ 0 & (\mathrm{mod}\,p) \quad 若 p-1\nmid n.\end{cases}$$

(e) 利用上面的结果或其它方法证明von Staudt-Clausen定理.

13．证明，如果$n\geqslant 2$，则Bernoulli多项式$B_n(x)$的导数是$nB_{n-1}(x)$.

14．证明，Bernoulli多项式满足加法公式

$$B_n(x+y)=\sum_{k=0}^{n}\binom{n}{k}B_k(x)y^{n-k}.$$

15．证明，Bernoulli多项式满足乘法公式

$$B_p(mx)=m^{p-1}\sum_{k=0}^{m-1}B_p\left(x+\frac{k}{m}\right).$$

16．证明，如果$r\geqslant 1$，则Bernoulli多项式满足

$$\sum_{k=0}^{r}\frac{2^{2k}B_{2k}}{(2k)!(2r+1-2k)!}=\frac{1}{(2r)!}.$$

17．用两种方法计算积分$\int_0^1 xB_p(x)dx$并推导出公式

$$\sum_{r=0}^{p}\binom{p}{r}\frac{B_r}{P+2-r}=\frac{B_{p+1}}{P+1}.$$

18. (a) 验证等式

$$\frac{uv}{(e^u-1)(e^v-1)}\quad\frac{e^{u+v}-1}{u+v}$$

$$=\frac{uv}{u+v}\left(1+\frac{1}{e^u-1}+\frac{1}{e^v-1}\right)$$

$$=1+\sum_{n=2}^{\infty}\frac{uv}{n!}\left(\frac{u^{n-1}+v^{n}-1}{u+v}\right)B_n.$$

(b) 令$J=\int_0^1 B_p(x)B_q(x)dx$，证明，J是(a)的展开式里$p!q!u^pv^q$的系数．由此推出

$$\int_0^1 B_p(x)B_q(x)dx$$

$$=\begin{cases}(-1)^{p-1}\dfrac{p!q!}{(q+p)!}B_{p+q} & \text{若}p\geqslant1,\ q\geqslant1,\\ 1 & \text{若}p=q=0,\\ 0 & \text{若}p\geqslant1\quad q=0\\ & \text{或}p=0\quad q\geqslant1.\end{cases}$$

19. (a) 用与18题类似的方法推导等式

$$(u+v)\sum_{m=0}^{\infty}\sum_{n=0}^{\infty}B_m(x)B_n(x)\frac{u^mv^n}{m!n!}$$

$$=\sum_{m=0}^{\infty}\sum_{n=0}^{\infty}B_{m+n}(x)\frac{u^mv^n}{m!n!}\sum_{r=0}^{\infty}\frac{B_{2r}}{(2r)!}(u^{2r}v+uv^{2r}).$$

(b) 比较(a)里的系数并利用其结果推导公式

$$B_m(x)B_n(x)$$

$$=\sum_r\left\{\binom{m}{2r}n+\binom{n}{2r}m\right\}\frac{B_{2r}B_{m+n-2r}(x)}{m+n-2r}$$

$$+(-1)^{m-1}\frac{m!n!}{(m+n)!}B_{m+n}$$

对$m\geqslant1$，$n\geqslant1$成立．并指出指标r的范围．

20．证明，如果$m\geqslant1$，$n\geqslant1$，$p\geqslant1$，则有

$$\int_0^1 B_m(x)B_n(x)B_p(x)dx$$

$$=(-1)^{p+1}p!\left\{\binom{m}{2r}n+\binom{n}{2r}m\right\}\frac{(m+n-2r-1)!}{(m+n+p-2r)!}$$

$$\times B_{2r}B_{m+n+p-2r}.$$

特别，由此公式计算$\int_0^1 B_2^3(x)dx$.

21．令$f(n)$是一个周期$\bmod k$的数论函数，并令

$$g(n)=\frac{1}{k}\sum_{m \bmod k} f(m)e^{\frac{-2\pi imn}{k}}$$

表示f的有限Fourier系数．如果

$$F(s)=k^{-s}\sum_{r=1}^{k} f(r)\zeta\left(s,\ \frac{r}{k}\right),$$

证明

$$F(1-s)=\frac{\Gamma(s)}{(2\pi)^s}\left\{e^{\frac{\pi is}{2}}\sum_{r=1}^{k} g(r)\zeta\left(s,\ \frac{r}{k}\right)\right.$$

$$\left.+e^{\frac{-\pi is}{2}}\sum_{r=1}^{k} g(-r)\zeta\left(s,\ \frac{r}{k}\right)\right\}.$$

22．令χ是模k的任一非本原特征，并令

$$S(x)=\sum_{n\leqslant x}\chi(n).$$

(a) 如果$N\geqslant1$，$\sigma>0$，证明

$$L(s,\ \chi)=\sum_{n=1}^{N}\frac{\chi(n)}{n^s}+s\int_N^{\infty}\frac{S(x)-S(N)}{x^{s+1}}dx$$

(b) 如果$s=\sigma+it$，$\sigma\geqslant\delta>0$，$|t|\geqslant0$．利用(a)，

证明存在一个常数$A(\delta)$，使得

$L(s, \chi)\leqslant A(\delta)B(k)(|t|+1)^{1-\delta}$，

其中$B(k)$是$|S(\chi)|$的一个上界.在定理13.15里已知

$B(k)=O(\sqrt{k}\log k)$.

(c) 证明，对某个常数$A>1$，我们有

$|L(s, \chi)|\leqslant A\log k$，当$\sigma\geqslant 1-\frac{1}{\log k}$且$0\leqslant|t|\leqslant 2$

时.[提示：在(a)里取$N=K$.]

第十三章　素数定理的解析证明

13.1　证明的方案

素数定理等价于

(1) $\psi(x) \sim x$　　当$x \to \infty$时，

其中$\psi(x)$是Chebysev函数

$$\psi(x) = \sum_{n \leq x} \Lambda(n).$$

本章给出一个以Riemann Eeta函数的性质为基础的(1)的一个解析证明. 此证明比第四章里的初等证明还短并且其主要思想易于理解. 本节概述证明的主要特点.

函数ψ是一个阶梯函数并且它的积分很便于讨论. 我们把它的积分记为ψ_1，即我们讨论

$$\psi_1(x) = \int_1^x \psi(t)dt.$$

积分ψ_1是一个分段连续函数. 首先我们证明，渐近关系式

(2) $\psi_1(x) \sim \frac{1}{2}x^2$　　当$x \to \infty$时

能推出(1)，然后再证明(2). 为此，我们用Riemann Zeta函数把$\frac{\psi_1(x)}{x^2}$表为一个围道积分的平均值，

$$\frac{\psi_1(x)}{x^2}=\frac{1}{2\pi i}\int_{c-\infty i}^{c+\infty i}\frac{x^{s-1}}{(s+1)}\left(-\frac{\zeta'(s)}{\zeta(s)}\right)ds,$$

其中$c>1$.

商$-\frac{\zeta'(s)}{\zeta(s)}$在$s=1$处有一个残数为1的一级极点，如果我们去掉这个极点，就得到

$$\frac{\psi_1(x)}{x^2}-\frac{1}{2}\left(1-\frac{1}{x}\right)^2$$

$$=\frac{1}{2\pi i}\int_{c-\infty i}^{c+\infty i}\frac{x^{s-1}}{s(s+1)}\left(-\frac{\zeta'(s)}{\zeta(s)}-\frac{1}{s-1}\right)ds,$$

对$c>1$.

我们令

$$h(s)=\frac{1}{s(+1)}\left(-\frac{\zeta'(s)}{\zeta(s)}-\frac{1}{s-1}\right)$$

并把上面的式子改写为

$$(3)\quad \frac{\psi_1(x)}{x^2}-\frac{1}{2}\left(1-\frac{1}{x}\right)^2=\frac{1}{2\pi i}\int_{c-\infty i}^{c+\infty i}x^{s-1}h(s)ds$$

$$=\frac{x^{c-1}}{2\pi}\int_{-\infty}^{+\infty}h(c+it)e^{it\log x}dt.$$

为了完成这个证明，我们必须证明

$$(4)\quad \lim_{x\to\infty}\frac{x^{c-1}}{2\pi}\int_{-\infty}^{+\infty}h(c+it)e^{it\log x}dt=0.$$

Fourier级数理论里的Riemann-Lebesgue引理可表示为

$$\lim_{x\to\infty}\int_{-\infty}^{+\infty}f(t)e^{itx}dt=0.$$

如果积分$\int_{-\infty}^{+\infty}|f(t)|\,dt$收敛的话. 把x换为$\log x$，(4)里的积分就是这种类型的积分，并且我们容易证明积分

$\int_{-\infty}^{+\infty}|h(c+it)|dt$对$c>0$收敛．所以，当$x\to\infty$时，(4)里的积分趋于0．但当$c>1$时，积分符号外面的因子$x^{c-1}$趋于$\infty$时，所以我们有一个不定式$\infty\cdot 0$．(3)对每一个$c>1$成立．如果在(3)里取$c=1$，令人讨厌的因子$x^{c-1}$将会消失，但$h(c+it)$变为$h(1+it)$而在直线$\sigma=1$上被积函数含有$\frac{\zeta'(s)}{\zeta(s)}$，此时，要证明积分$\int_{-\infty}^{+\infty}|h(1+it)|dt$收敛更困难．在验证收敛性之前我们必须应用Riemann-Lebesgue引理．证明的最后部分也是更困难的部分是证明在(3)里可以用1去代替c，并且积分$\int_{-\infty}^{+\infty}|h(1+it)|dt$收敛．这需要更详细地研究直线$\sigma=1$附近的Riemann zeta函数．

现在我们开始实施上述计划，我们先从几个引理开始．

13.2 引理

引理 1 对任一数论函数$a(n)$，令

$$A(x)=\sum_{n\leq x}a(n),$$

如果$x<1$，令$A(x)=0$，则有

$$(5)\quad \sum_{n\leq x}(x-n)a(n)=\int_1^x A(t)dt.$$

证明 如果f在[1，x]上有连续导数，我们应用Abel等式(定理4.2.)，有

$$(6)\quad \sum_{n\leq x}a(n)f(n)=A(x)f(x)-\int_1^x A(t)f'(t)dt.$$

取$f(t)=t$，我们有

$$\sum_{n\leqslant x} a(n)f(n)=\sum_{n\leqslant x} na(n) \text{与} A(x)f(x)=x\sum_{n\leqslant x} a(n),$$

所以(6)化为(5). □

下面的引理是分段递增线性函数的L'Hôspital规则的一种形式.

引理 2 令$A(x)=\sum_{n\leqslant x} a(n)$，$A_1(x)=\int_1^x A(t)dt$，并设$a(n)\geqslant 0$，对所有的n. 如果对某个$c>0$与$L>0$，我们有渐近公式

(7) $A_1(x)\sim Lx^c$ 当$x\to\infty$时，

那么我们有

(8) $A(x)\sim cLx^{c-1}$ 当$x\to\infty$时.

换言之，由(7)的形式微分给出一个正确的结果.

证明 因为$a(n)$非负，所以函数$A(x)$是递增的. 选取任一$\beta>1$并考虑差$A_1(\beta x)-A_1(x)$，我们有

$$\begin{aligned}A_1(\beta x)-A_1(x)&=\int_x^{\beta x} A(u)du\geqslant\int_x^{\beta x} A(x)du\\&=A(x)(\beta x-x)\\&=x(\beta-1)A(x).\end{aligned}$$

这给我们

$$xA(x)\leqslant\frac{1}{\beta-1}\{A_1(\beta x)-A_1(x)\}$$

或者

$$\frac{A(x)}{x^{c-1}}\leqslant\frac{1}{\beta-1}\left\{\frac{A_1(\beta x)}{(\beta x)^c}\beta^c-\frac{A_1(x)}{x^c}\right\}.$$

在这个不等式中，保持β不变并令$x\to\infty$，得

$$\limsup_{x\to\infty}\frac{A(x)}{x^{c-1}}\leqslant\frac{1}{\beta-1}(L\beta^c-L)=L\frac{\beta^c-1}{\beta-1}.$$

现在令$\beta\to 1_+$，右端的商是在$x=1$时x^c的导数的差商并有极限c，因此有

$$(9)\quad \limsup_{x\to\infty}\frac{A(x)}{x^{c-1}}\leqslant cL.$$

现在考虑$0<\alpha<1$中的任一α，并考虑$A_1(x)-A_1(\alpha x)$. 同上面的理由类似，可推出

$$\liminf_{x\to\infty}\frac{A(x)}{x^{c-1}}\geqslant L\ \frac{1-\alpha^c}{1-\alpha}.$$

当$\alpha\to 1-$时，右端趋于cL，这与(9)一起，证明了$\frac{A(x)}{x^{c-1}}$趋于极限cL，当$x\to\infty$时. □

当$a(n)=\Lambda(n)$时，我们有$A(x)=\psi(x)$，$A_1(x)=\psi_1(x)$，并且$a(n)\geqslant 0$. 因此，应用引理1与引理2立即得

定理13.1　我们有

$$(10)\quad \psi_1(x)=\sum_{n\leqslant x}(x-n)\Lambda(n).$$

还有，当$x\to\infty$时，渐近关系式$\psi_1(x)\sim\frac{x^2}{2}$可推出$\psi(x)\sim x$.

下面的工作是把$\frac{\psi_1(x)}{x^2}$表示为一个包含有zeta函数的积分. 为此，我们需要下面的关于围道积分的引理的特殊情形$k=1$与$k=2$.（与第十一章引理4比较.）

引理3　如果$c>0$，$u>0$，那么对任意的整数$k\geqslant 1$，我们有

$$\frac{1}{2\pi i}\int_{c-\infty i}^{c+\infty i}\frac{u^{-z}}{z(z+1)\cdots(z+k)}dz$$

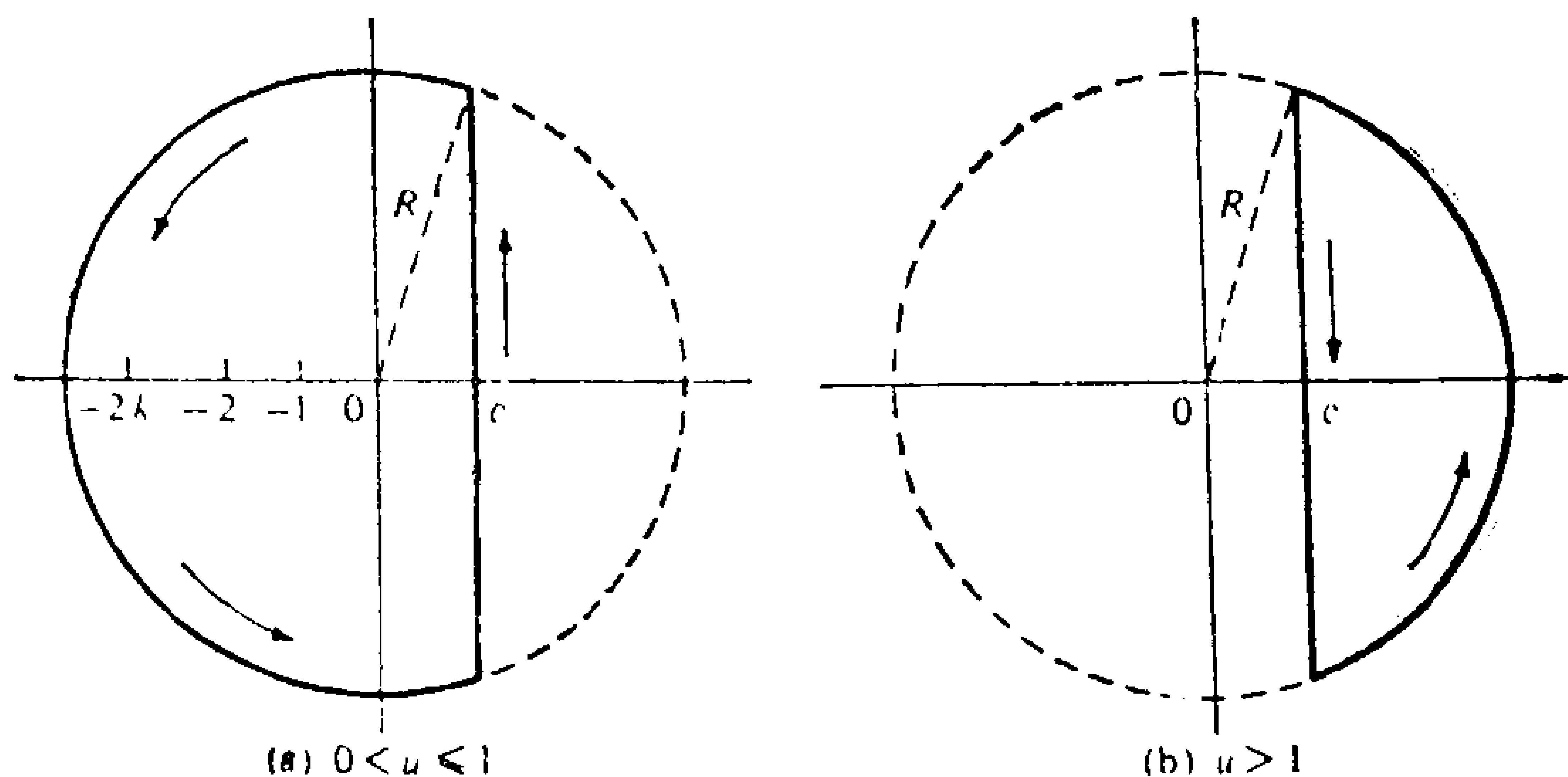
$$=\begin{cases}\frac{1}{k!}(1-u)^k & 若0<u\leqslant 1,\\ 0 & 若u>1,\end{cases}$$

这个积分是绝对收敛的.

证明　首先我们注意，被积函数等于$\frac{u^{-z}\Gamma(z)}{\Gamma(z+k+1)}$，这是反复多次利用函数方程$\Gamma(z+1)=z\Gamma(z)$而得. 为了证明此引理，我们对积分

$$\frac{1}{2\pi i}\int_{c(R)}\frac{u^{-z}\Gamma(z)}{\Gamma(z+k+1)}dz$$

应用Cauchy残数定理. 其中$c(R)$是围道，当$0<u\leqslant 1$时，如图13.1(a)所示；当$u>1$时，如图13.1(b)所示. 由于圆半径R大于$2k+c$，所以，所有的极点$z=0, -1, \cdots, -k$都在圆的内部.



（图13.1）

现在，我们证明，当$R\to\infty$时，沿着每一个圆弧的积分趋于0. 如果$z=x+iy$并且$|z|=R$，则被积函数不超过

$$\left|\frac{u^{-z}}{z(z+1)\cdots(z+k)}\right|=\frac{u^{-x}}{|z|\,|z+1|\cdots|z+k|}$$

$$\leqslant\frac{u^{-c}}{R|z+1|\cdots|z+k|}.$$

当$0<u\leq 1$时，u^{-x}是递增函数，当$u>1$时，u^{-x}是递减函数，由此即得$u^{-x}\leq u^{-c}$. 如果$1\leq n\leq k$，则有

$$|z+n|\geq|z|-n=R-n\geq R-k\geq\frac{R}{2}$$

这因为$R>2k$. 因此，沿每一圆弧的积分不超过

$$\frac{2\pi Ru^{-c}}{R\left(\frac{1}{2}R\right)^{k}}=0(R^{-k}),$$

并因$k\geq 1$，所以当$R\to\infty$时，上式$\to 0$.

如果$u>1$，被积函数在$c(R)$内部是解析的，于是$\int_{c(R)}=0$. 令$R\to\infty$，在此情况下，引理得到证明.

如果$0<u\leq 1$，我们根据Cauchy残数定理来估算沿$c(R)$的积分的值. 被积函数在整数$n=0, -1, \cdots, -k$处有极点，于是

$$\frac{1}{2\pi i}\int_{c(R)}\frac{u^{-z}\Gamma(z)}{\Gamma(z+k+1)}dz$$

$$=\sum_{n=0}^{k}\operatorname{Res}_{z=-n}\frac{u^{-z}\Gamma(z)}{\Gamma(z+k+1)}$$

$$=\sum_{n=0}^{k}\frac{u^{n}}{\Gamma(k+1-n)}\operatorname{Res}_{z=-n}\Gamma(z)=\sum_{n=0}^{k}\frac{u^{n}(-1)^{n}}{(k-n)!n!}$$

$$=\frac{1}{k!}\sum_{n=0}^{k}\binom{k}{n}(-u)^{n}=\frac{(1-u)^{k}}{k!}.$$

令$R\to\infty$，即得引理. □

13.3 $\frac{\psi_1(x)}{x^2}$的围道积分表示

定理13.2 如果$c>1$，$x\geq 1$，则有

$$(11)\quad \frac{\psi_1(x)}{x^2}=\frac{1}{2\pi i}\int_{c-\infty i}^{c+\infty i}\frac{x^{s-1}}{s(s+1)}\left(-\frac{\zeta'(s)}{\zeta(s)}\right)ds.$$

证明　由等式(10)，我们有$\dfrac{\psi_1(x)}{x}=\sum\limits_{n\leqslant x}\left(1-\dfrac{n}{x}\right)\Lambda(n)$.

利用引理3，令其中$k=1$，$u=\dfrac{n}{x}$. 如果$n\leqslant x$，我们得

$$1-\frac{n}{x}=\frac{1}{2\pi i}\int_{c-\infty i}^{c+\infty i}\frac{\left(\frac{x}{n}\right)^s}{s(s+1)}ds,$$

用$\Lambda(n)$去乘此式，并对所有$n\leqslant x$求和，得

$$\frac{\psi_1(x)}{x}=\sum_{n\leqslant x}\frac{1}{2\pi i}\int_{c-\infty i}^{c+\infty i}\frac{\Lambda(n)\left(\frac{x}{n}\right)^s}{s(s+1)}ds$$

$$=\sum_{n=1}^{\infty}\frac{1}{2\pi i}\int_{c-\infty i}^{c+\infty i}\frac{\Lambda(n)\left(\frac{x}{n}\right)^s}{s(s+1)}ds,$$

这因为当$n>x$时，积分为0，上式还可写为

$$(12)\quad \frac{\psi_1(x)}{x}=\sum_{n=1}^{\infty}\int_{c-\infty i}^{c+\infty i}f_n(s)ds,$$

其中$2\pi i f_n(x)=\dfrac{\Lambda(n)\left(\frac{x}{n}\right)^s}{(s^2+s)}$. 下面我们想交换(12)中和与积分的位置，为此，只要证明级数

$$(13)\quad \sum_{n=1}^{\infty}\int_{c-\infty i}^{c+\infty i}|f_n(s)|ds$$

收敛即可. （参阅[2]里的定理10.26.）此级数的部分和满足不等式

$$\sum_{n=1}^{N}\int_{c-\infty i}^{c+\infty i}\frac{\Lambda(n)\left(\frac{x}{n}\right)^{c}}{|s||s+1|}ds$$

$$=\sum_{n=1}^{N}\frac{\Lambda(n)}{n^{c}}\int_{c-\infty i}^{c+\infty i}\frac{x^{c}}{|s||s+1|}ds$$

$$\leqslant A\sum_{n=1}^{\infty}\frac{\Lambda(n)}{n^{c}},$$

其中A是一个常数，所以(13)收敛．于是我们能够交换(12)中的和与积分符号而得

$$\frac{\psi_1(x)}{x}=\int_{c-\infty i}^{c+\infty i}\sum_{n=1}^{\infty}f_n(s)ds$$

$$=\frac{1}{2\pi i}\int_{c-\infty i}^{c+\infty i}\frac{x^{s}}{s(s+1)}\sum_{n=1}^{\infty}\frac{\Lambda(n)}{n^{s}}ds$$

$$=\frac{1}{2\pi i}\int_{c-\infty i}^{c+\infty i}\frac{x^{s}}{s(s+1)}\left(-\frac{\zeta'(s)}{\zeta(s)}\right)ds.$$

两端同除以x，即得(11)． □

定理13.3　如果$c>1$，$x\geqslant1$，则有

(14) $$\frac{\psi_1(x)}{x^2}-\frac{1}{2}\left(1-\frac{1}{x}\right)^2=\frac{1}{2\pi i}\int_{c-\infty i}^{c+\infty i}x^{s-1}h(s)ds,$$

其中

(15) $$h(s)=\frac{1}{s(s+1)}\left(-\frac{\zeta'(s)}{\zeta(s)}-\frac{1}{s-1}\right).$$

证明　我们利用引理3，令其中$k=2$，得

$$\frac{1}{2}\left(1-\frac{1}{x}\right)^2=\frac{1}{2\pi i}\int_{c-\infty i}^{c+\infty i}\frac{x^{s}}{s(s+1)(s+2)}ds,$$

其中$c>0$．在积分里，用$s-1$代替s（保持$c>1$），并由(11)减去上式即得本定理． □

如果我们把积分路线写为参数形式$s=c+it$，我们得到$x^{s-1}=x^{c-1}x^{it}=x^{c-1}e^{it\log x}$，(14)式变为

$$(16)\quad \frac{\psi_1(x)}{x^2}-\frac{1}{2}\left(1-\frac{1}{x}\right)^2 = \frac{x^{c-1}}{2}\int_{c-\infty i}^{c+\infty i} h(c+it)e^{it\log x}dt.$$

下面的工作是证明，当$x\to\infty$时，(16)的右端趋于0．如前所述，我们首先证明，在(16)里我们能够使$c=1$．为此我们需要研究在直线$\sigma=1$附近$\zeta(s)$的情况．

13.4 直线$\sigma=1$附近$|\zeta(s)|$与$|\zeta'(s)|$的上界

为研究在直线$\sigma=1$附近$\zeta(s)$的情况，我们利用定理12.21得到的表示式，它对于$\sigma>0$是成立的，

$$(17)\quad \zeta(s)=\sum_{n=1}^{N}\frac{1}{n^s}-s\int_N^\infty \frac{x-[x]}{x^{s+1}}dx+\frac{N^{1-s}}{s-1}.$$

我们还要利用对(17)两边微分得到的$\zeta'(s)$的公式

$$(18)\quad \zeta'(s)=-\sum_{n=1}^{N}\frac{\log n}{n^s}+s\int_N^\infty \frac{(x-[x])\log x}{x^{s+1}}dx - \int_N^\infty \frac{x-[x]}{x^{s+1}}dx-\frac{N^{1-s}\log N}{s-1} - \frac{N^{1-s}}{(s-1)^2}.$$

下面的定理利用这两个式子得到$|\zeta(s)|$与$|\zeta'(s)|$的上界．

定理13.4　对每一个$A>0$，存在一个常数M（依赖于A）使得

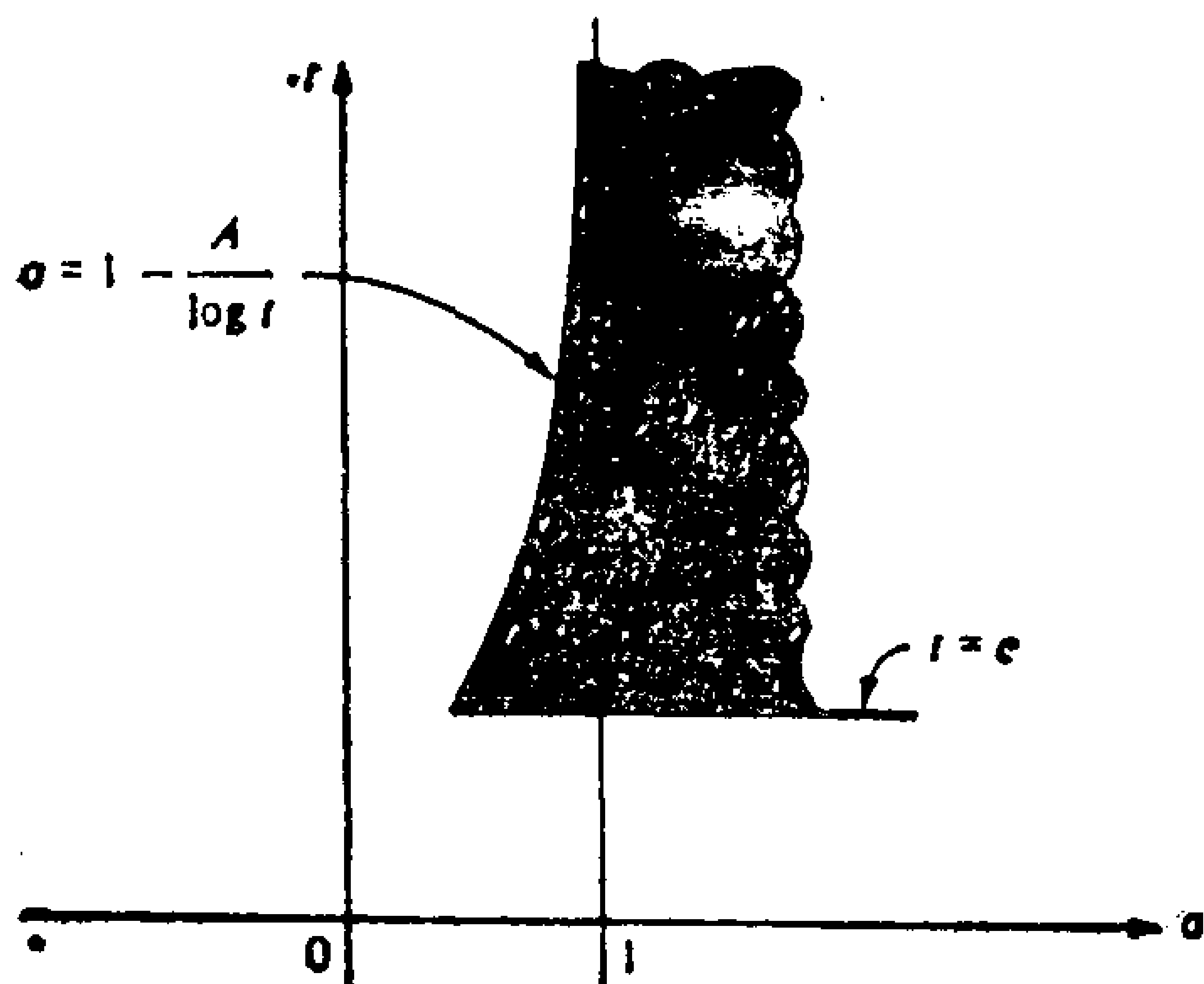
(19)　$|\zeta(s)|\leqslant M\log t$与$|\zeta'(s)|\leqslant M\log^2 t$

对于$\sigma\geqslant\frac{1}{2}$并满足

$$(20)\quad \sigma > 1 - \frac{A}{\log t} \quad t \geqslant e$$

的所有的s成立．

注意：不等式(20)描绘出一个如图13.2所示的区域．



（图13.2）

证明　如果$\sigma \geqslant 2$，则有$|\zeta(s)| \leqslant \zeta(2)$，$|\zeta'(s)| \leqslant |\zeta'(2)|$，因而(19)中两个不等式是成立的．因此我们假设$\sigma < 2$，$t \geqslant e$，于是有

$$|s| \leqslant \sigma + t \leqslant 2 + t < 2t \text{且} |s-1| \geqslant t$$

所以$\frac{1}{|s-1|} \leqslant \frac{1}{t}$．利用(17)，估算$|\zeta(s)|$，得

$$|\zeta(s)| \leqslant \sum_{n=1}^{N} \frac{1}{n^{\sigma}} + 2t\int_{N}^{\infty} \frac{1}{x^{\sigma+1}} dx + \frac{N^{1-\sigma}}{t}$$

$$= \sum_{n=1}^{N} \frac{1}{n^{\sigma}} + \frac{2t}{\sigma N^{\sigma}} + \frac{N^{1-\sigma}}{t}.$$

取$N = [t]$，则有$N \leqslant t < N+1$．若$n \leqslant N$，则$\log n \leqslant \log t$．不等式(20)即$1 - \sigma < \frac{A}{\log t}$，所以

$$\frac{1}{n^{\sigma}}=\frac{n^{1-\sigma}}{n}=\frac{1}{n}e^{(1-\sigma)\log n}<\frac{1}{n}e^{\frac{A\log n}{\log t}}\leqslant\frac{1}{n}e^{A}$$

$$=0\left(\frac{1}{n}\right).$$

因此,

$$\frac{2t}{\sigma N^{\sigma}}\leqslant\frac{N+1}{N}=0(1),$$

$$\frac{N^{1-\sigma}}{t}=\frac{N}{t}\frac{1}{N^{\sigma}}=0\left(\frac{1}{N}\right)=0(1),$$

所以,

$$|\zeta(s)|=0\left(\sum_{n=1}^{N}\frac{1}{n}\right)+0(1)=0(\log N)+0(1)$$

$$=0(\log t).$$

这证明了(19)式中关于$|\zeta(s)|$的不等式是成立的. 为得到$|\zeta'(s)|$的不等式, 我们对(18)应用类似的理由, 唯一的差别是右端出现一个特别的因子$\log N$, 但$\log N=0(\log t)$, 所以在这个特定的区域里, 我们得到$|\zeta'(s)|=0(\log^2 t)$.

13.5 在直线$\sigma=1$上$\zeta(s)$不为零

这一节, 我们证明, 对每一个实数t, $\zeta(1+it)\neq 0$. 这个证明基于一个不等式, 这个不等式在下一节还要用到.

定理13.5 如果$\sigma>1$, 我们有

(21) $\zeta^3(\sigma)|\zeta(\sigma+it)|^4|\zeta(\sigma+2it)|\geqslant 1$.

证明 我们回到在11.9节的例1里证明过的等式$\zeta(s)=e^{G(s)}$, 其中

$$G(s)=\sum_{n=2}^{\infty}\frac{\Lambda(n)}{\log n}n^{-s}=\sum_{p}\sum_{m=1}^{\infty}\frac{1}{mp^{ms}}\ (\sigma>1).$$

这能改写为

$$\zeta(s)=\exp\left\{\sum_{p}\sum_{m=1}^{\infty}\frac{1}{mp^{ms}}\right\}$$

$$=\exp\left\{\sum_{p}\sum_{m=1}^{\infty}\frac{e^{-itm\log p}}{mp^{m\sigma}}\right\},$$

由此可得

$$|\zeta(s)|=\exp\left\{\sum_{p}\sum_{m=1}^{\infty}\frac{\cos(mt\log p)}{mp^{m\sigma}}\right\}.$$

对$s=\sigma$，$s=\sigma+it$，$s=\sigma+2it$ 我们多次应用这个公式，得

$$\zeta^{3}(s)|\zeta(\sigma+it)|^{4}|\zeta(\sigma+2it)|$$

$$=\exp\left\{\sum_{p}\sum_{m=1}^{\infty}\frac{3+4\cos(mt\log p+\cos(2mt\log p)}{mp^{m\sigma}}\right\}.$$

但我们有三角不等式

$$3+4\cos\theta+\cos2\theta\geqslant0,$$

它是由等式

$$3+4\cos\theta+\cos2\theta=3+4\cos\theta+2\cos^{2}\theta-1$$

$$=2(1+\cos\theta)^{2}$$

得到的．因此，最后的无穷级数里的每一项都是非负的，所以我们得到（21）． □

定理13.6　对每一个实数t都有$\zeta(1+it)\neq0$.

证明　我们只需讨论$t\neq0$．(21)可改写为

$$(22)\quad \{(\sigma-1)\zeta(\sigma)\}^{3}\left|\frac{\zeta(\sigma+it)}{\sigma-1}\right|^{4}|\zeta(\sigma+2it)|\geqslant\frac{1}{\sigma-1},$$

这对于$\sigma>1$是正确的．于是在(22)里，令$\sigma\to1_{+}$，因为$\zeta(s)$

在极点$s=1$处有残数1，所以第一个因子趋于1，第三个因子趋于$|\zeta(1+2it)|$. 如果$\zeta(1+it)$等于0，那么中间的因子能写为

$$\left|\frac{\zeta(\sigma+it)-\zeta(1+it)}{\sigma-1}\right|^4\to|\zeta'(1+it)|^4$$

当$\sigma\to1_+$时.

因此，如果对某个$t\neq0$，有$\zeta(1+it)=0$，那么，当$\sigma\to1_+$时，(22)的左端趋于$|\zeta'(1+it)|^4|\zeta(1+2it)|$，而右端趋于$\infty$，这是一个矛盾. □

13.6 $\left|\frac{1}{\zeta(s)}\right|$与$\left|\frac{\zeta'(s)}{\zeta(s)}\right|$的不等式

我们再一次应用定理13.5可得下面的$\left|\frac{1}{\zeta(s)}\right|$与$\left|\frac{\zeta'(s)}{\zeta(s)}\right|$的不等式.

定理13.7 存在一个常数$M>0$，使得

$$\left|\frac{1}{\zeta(s)}\right|<M\log^7 t,\quad \left|\frac{\zeta'(s)}{\zeta(s)}\right|<M\log^9 t,$$

其中$\sigma\geq1$，$t\geq e$.

证明 对$\sigma\geq2$，我们有

$$\left|\frac{1}{\zeta(s)}\right|=\left|\sum_{n=1}^{\infty}\frac{\mu(n)}{n^s}\right|\leqslant\sum_{n=1}^{\infty}\frac{1}{n^2}\leqslant\zeta(2),$$

$$\left|\frac{\zeta'(s)}{\zeta(s)}\right|\leqslant\sum_{n=1}^{\infty}\frac{\Lambda(n)}{n^2},$$

所以，如果$\sigma\geq2$，定理中的两个不等式自然是成立的. 于是

假设$1\leqslant\sigma\leqslant 2$，$t\geqslant e$，不等式(21)改写为

$$\frac{1}{|\zeta(\sigma+it)|}\leqslant\zeta(\sigma)^{\frac{3}{4}}|\zeta(\sigma+2it)|^{\frac{1}{4}}.$$

而$(\sigma-1)\zeta(\sigma)$在区间$1\leqslant\sigma\leqslant 2$内是有界的，即$(\sigma-1)\zeta(\sigma)\leqslant M$，这里M是一个绝对常数，于是

$$\zeta(\sigma)\leqslant\frac{M}{\sigma-1}\quad 当1<\sigma\leqslant 2时.$$

如果$1\leqslant\sigma\leqslant 2$，则$\zeta(\sigma+2it)=0(\log t)$（根据定理13.4），所以，对$1<\sigma\leqslant 2$，我们有

$$\frac{1}{|\zeta(\sigma+it)|}\leqslant\frac{M^{\frac{3}{4}}(\log t)^{\frac{1}{4}}}{(\sigma-1)^{\frac{3}{4}}}=\frac{A(\log t)^{\frac{1}{4}}}{(\sigma-1)^{\frac{3}{4}}},$$

其中A是一个绝对常数. 因此对某个常数$\beta>0$，我们有

$$(23)\quad |\zeta(\sigma+it)|>\frac{B(\sigma-1)^{\frac{3}{4}}}{(\log t)^{\frac{1}{4}}}，若1<\sigma\leqslant 2，t\geqslant e.$$

这个式子对$\sigma=1$当然也成立. 令α是满足$1<\alpha<2$的任意一数，那么，如果$1\leqslant\sigma\leqslant\alpha$，$t\geqslant\alpha$，利用定理13.4，可写

$$\begin{aligned}|\zeta(\sigma+it)-\zeta(\alpha+it)|&\leqslant\int_\sigma^\alpha|\zeta'(u+it)|du\\&\leqslant(\alpha-\sigma)M\log^2 t\\&\leqslant(\alpha-1)M\log^2 t.\end{aligned}$$

于是，根据三角不等式，

$$\begin{aligned}|\zeta(\sigma+it)|&\geqslant|\zeta(\alpha+it)|-|\zeta(\sigma+it)-\zeta(\alpha+it)|\\&\geqslant|\zeta(\alpha+it)|-(\alpha-1)M\log^2 t\\&\geqslant\frac{B(\alpha-1)^{\frac{3}{4}}}{(\log t)^{\frac{1}{4}}}-(\alpha-1)M\log^2 t.\end{aligned}$$

这对于$1\leqslant\sigma\leqslant\alpha$是成立的，并根据(23)，对于$\alpha\leqslant\sigma\leqslant 2$也成

立，因为 $(\sigma-1)^{\frac{3}{4}}\geqslant(\alpha-1)^{\frac{3}{4}}$. 即，如果$1\leqslant\sigma\leqslant2$，$t\geqslant e$，我们有，不等式

$$|\zeta(\sigma+it)|\geqslant\frac{B(\alpha-1)^{\frac{3}{4}}}{(\log t)^{\frac{1}{4}}}-(\alpha-1)M\log^2 t$$

对任一满足$1<\alpha<2$的α成立，现在我们作一个依赖于t的α，使上式右边第一项是第二项的两倍，这要求

$$\alpha=1+\left(\frac{B}{2M}\right)^4\frac{1}{(\log t)^9}.$$

显然，如果对某个t_0，有$t\geqslant t_0$，则$\alpha>1$且$\alpha<2$. 即，如果$t\geqslant t_0$，$1\leqslant\sigma\leqslant2$，则有

$$|\zeta(\sigma+it)|\geqslant(\alpha-1)M\log^2 t=\frac{c}{(\log t)^7}.$$

如果$e\leqslant t\leqslant t_0$，这个不等式也许对一个不同的$c$成立. 这证明，$|\zeta(s)|\geqslant c\log^{-7}t$对所有的$\sigma\geqslant1$，$t\geqslant e$成立. 这就给出$\left|\frac{1}{\zeta(s)}\right|$的相应的上界. 为了得到$\left|\frac{\zeta'(s)}{\zeta(s)}\right|$的不等式，我们应用定理13.4就得到一个外加的因子$\log^2 t$. □

13.7 素数定理证明的完成

现在我们即将完成素数定理的证明. 我们需要复变函数理论中的另一个事实，我们把它表述为一个引理.

引理 4 如果$f(s)$在$s=\alpha$处有一个k级极点，那么商$\frac{f'(s)}{f(s)}$在$s=k$处有一个残数为$-k$的一级极点.

证明　我们有$f(s)=\frac{g(s)}{(s-\alpha)^k}$，其中g在α处是解析的且$g(\alpha)\neq 0$．于是对于在α的一个邻域内的所有的s，我们有

$$f'(s)=\frac{g'(s)}{(s-\alpha)^k}-\frac{kg(s)}{(s-\alpha)^{k+1}}$$
$$=\frac{g(s)}{(s-\alpha)^k}\left\{\frac{-k}{s-\alpha}+\frac{g'(s)}{g(s)}\right\},$$

即

$$\frac{f'(s)}{f(s)}=-\frac{k}{s-\alpha}+\frac{g'(s)}{g(s)}.$$

因为$\frac{g'(s)}{g(s)}$在α处是解析的，引理得证．　□

定理13.8　函数

$$F(s)=-\frac{\zeta'(s)}{\zeta(s)}-\frac{1}{s-1}$$

在$s=1$处是解析的．

证明　根据引理4，$-\frac{\zeta'(s)}{\zeta(s)}$与$\frac{1}{(s-1)}$在点1处都有残数为1的一级极点，所以，它们的差在$s=1$处是解析的．　□

定理13.9　对$x\geqslant 1$，我们有

$$\frac{\psi_1(x)}{x^2}-\frac{1}{2}\left(1-\frac{1}{x}\right)^2$$
$$=\frac{1}{2\pi}\int_{-\infty}^{\infty}h(1+it)e^{it\log x}dt$$

其中积分$\int_{-\infty}^{\infty}|h(1+it)|dt$收敛．因此，根据Riemann-Lebesgue引理，我们有

(24) $\psi_1(x)\sim\frac{x^2}{2}$，

于是有

$$\psi(x) \sim x \quad \text{当} x \to \infty \text{时}.$$

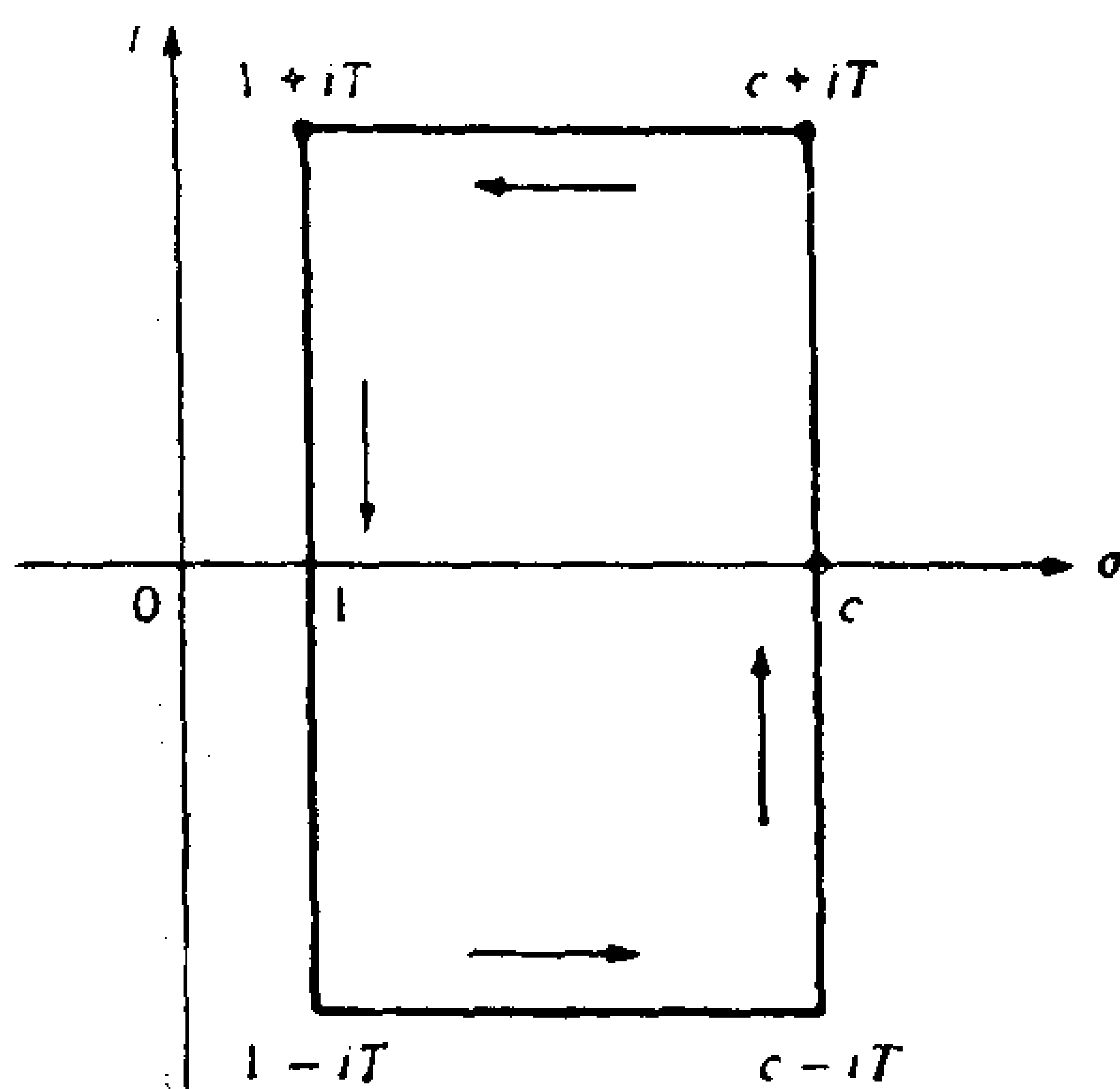
证明 在定理13.3里我们证明过，当$c>1$，$x \geqslant 1$时，我们有

$$\frac{\psi_1(x)}{x^2} - \frac{1}{2}\left(1-\frac{1}{x}\right)^2 = \frac{1}{2\pi i}\int_{c-\infty i}^{c+\infty i} x^{s-1} h(s)\,ds,\ ,$$

其中

$$h(s) = \frac{1}{s(s+1)}\left(-\frac{\zeta'(s)}{\zeta(s)} - \frac{1}{s-1}\right).$$

我们的首要任务是证明，我们可以把积分路线移动到$\sigma=1$。为此，我们对图13.3里所示的矩形R应用Cauchy定理．$x^{s-1}h(s)$沿R的积分是0，因为被积函数在R内部与R上是解析的．



（图13.3）

现在我们证明，当$T\to\infty$时，沿水平路线的积分趋于0．因为被积函数在共轭点处有相同的绝对值，所以只讨论上面部分就够了，$t=T$．在这一部分，我们有估计式

$$\left|\frac{1}{s(s+1)}\right| \leqslant \frac{1}{T^2}\text{与}$$

$$\left|\frac{1}{s(s+1)(s-1)}\right| \leqslant \frac{1}{T^3} \leqslant \frac{1}{T^2}.$$

还有，存在一个常数M，使得，当$\sigma \geqslant 1$，$t \geqslant e$时，$\left|\frac{\zeta'(s)}{\zeta(s)}\right| \leqslant M$．于是，当$T \geqslant e$时，我们有

$$|h(s)| \leqslant \frac{M\log^9 T}{T^2},$$

所以

$$\left|\int_1^c x^{s-1}h(s)ds\right| \leqslant \int_1^c x^{c-1}\frac{M\log^9 T}{T^2}d\sigma$$

$$= Mx^{c-1}\frac{\log^9 T}{T^2}(c-1).$$

因此，当$T\to\infty$时，沿水平线段的积分趋于0， 于是我们有

$$\int_{c-\infty i}^{c+\infty i} x^{s-1}h(s)ds = \int_{1-\infty i}^{1+\infty i} x^{s-1}h(s)ds.$$

在直线$\sigma=1$上我们写$S=1+it$，得

$$\frac{1}{2\pi i}\int_{1-\infty i}^{1+\infty i} x^{s-1}h(s)ds$$

$$=\frac{1}{2\pi}\int_{-\infty}^{\infty} h(1+it)e^{iT\log x}dt.$$

我们注意到

$$\int_{-\infty}^{\infty}|h(1+it)|dt = \int_{-e}^{e} + \int_{e}^{\infty} + \int_{-\infty}^{-e}.$$

在从e到∞的积分里，我们有

$$|h(1+it)| \leqslant \frac{M\log^9 t}{t^2},$$

所以$\int_e^\infty |h(1+it| dt$收敛．类似地，$\int_{-\infty}^{e}$收敛，所以$\int_{-\infty}^{\infty}|h(1+it)|dt$收敛．即，我们能应用Riemann-Lebesgue引理得到$\psi_1(x)\sim\frac{x^2}{2}$．根据定理13.1，这推出$\psi(x)\sim x$当$x\to\infty$时．素数定理的证明全部完成． □

13.8 ζ(s)的无零点区域

在定理13.7里被我们证明过的对$\sigma\geqslant 1$，$t\geqslant e$成立的不等

式$\left|\frac{1}{\zeta(s)}\right|<M\log^7 t$能扩大到直线$\sigma=1$的左边．这个不等式在一个带形区域里不能得到，这个区域与图13.2里所示的图形有些相似，其中左边界曲线在$t\to\infty$时逐渐靠近直线$\sigma=1$．这个不等式意味着，在这个区域里$\zeta(s)$不为零．更确切地说，我们有

定理13.10　设$\sigma\geqslant\frac{1}{2}$，则存在常数$A>0$与$C>0$，使得

$$|\zeta(\sigma+it)|>\frac{C}{\log^7 t},$$

其中

$$(25)\quad 1-\frac{A}{\log^9 t}<\sigma\leqslant 1 \text{ 且 } t\geqslant e,$$

这推出，如果σ与t满足(25)，则$\zeta(\sigma+it)\neq 0$

证明　利用三角不等式与定理13.7，得出

$$(26)\quad |\zeta(\sigma+it)|\geqslant|\zeta(1+it)|-|\zeta(1+it)-\zeta(\sigma+it)|$$
$$>\frac{B}{\log^7 t}-|\zeta(1+it)-\zeta(\sigma+it)|,$$

对某个$B>0$成立．为估计最后一项，我们写

$$|\zeta(1+it)-\zeta(\sigma+it)|=\left|\int_\sigma^1\zeta'(u+it)du\right|$$
$$\leqslant\int_\sigma^1|\zeta'(u+it)|du$$

因为$t\geqslant e$，我们有$\log^9 t\geqslant\log t$，所以$1-\left(\frac{A}{\log^9 t}\right)\geqslant 1-\left(\frac{A}{\log t}\right)$，即，如果$\sigma$对任一$A>0$满足(25)，则我们能应用定理13.4对$|\zeta'(u+it)|$的估计式，得

$$|\zeta(1+it)-\zeta(\sigma+it)|\leqslant M(1-\sigma)\log^2 t$$

$$<M\log^2 t\frac{A}{\log^9 t}=\frac{MA}{\log^7 t}.$$

在(26)里利用此式，得

$$|\zeta(\sigma+it)|>\frac{B-MA}{\log^7 t},$$

对某个$B>0$、任一$A>0$与某个依赖于A的$M>0$成立．M的值由某个A或某个任意小的A来确定．因此，我们能够选择充分小的A，使得$B-MA>0$．如果我们令$C=B-MA$，那么最后的不等式变为$|\zeta(\sigma+it)|>c\log^{-7}t$，这证明了对所有满足

$$1-\frac{A}{\log^9 t}<\sigma<1\text{与}t\geq e$$

的σ与t，定理成立．又根据定理13.7，这个结果对$\sigma=1$也成立，于是证明完成．□

我们知道，如果$\sigma\geqslant 1$，则$\zeta(s)\neq 0$，并且由函数方程

$$\zeta(s)=2(2\pi)^{1-s}\Gamma(1-s)\sin\left(\frac{\pi s}{2}\right)\zeta(1-s)$$

看出，如果$\sigma\leqslant 0$，除开零点$s=-2,\ -4,\ -6,\ \cdots$之外，都有$\zeta(s)\neq 0$，这些零点是由$\sin\left(\frac{\pi s}{2}\right)$为零而产生的，这些零点称为“平凡”零点，下面的定理指出，除开平凡零点之外，在实轴上，$\zeta(s)$没有其它的零点．

定理13.11　如果$\sigma>0$，则有

$$(27)\quad (1-2^{1-s})\zeta(s)=\sum_{n=1}^{\infty}\frac{(-1)^{n-1}}{n^s}.$$

这就是说，如果s是实数并且$0<s<1$，则$\zeta(s)<0$．

证明　首先，设$\sigma>1$，于是有

$$(1-2^{1-s})\zeta(s)=\sum_{n=1}^{\infty}\frac{1}{n^s}-2\sum_{n=1}^{\infty}\frac{1}{(2n)^s}$$
$$=(1+2^{-s}+3^{-s}+\cdots)-2(2^{-s}+4^{-s}+6^{-s}+\cdots)$$
$$=1-2^{-s}+3^{-s}-4^{-s}+5^{-s}-6^{-s}+\cdots,$$

这证明了(27)对$\sigma>1$成立．如果$\sigma>0$，则右边的级数收敛，所以根据解析开拓，(27)对$\sigma>0$也成立．

当s是实数时，(27)里的级数是一个交错级数，其和为正数．如果$0<s<1$，则因子$(1-2^{1-s})$是负的，于是$\zeta(s)$也是负的．

13.9 Riemann假设

Riemann在1859年出版的8页著名的关于$\pi(x)$的论文[58]中指出，$\zeta(s)$的非平凡零点看来都在直线$\sigma=\frac{1}{2}$上，尽管他没能证明这一点．所有非平凡零点都有实部$\frac{1}{2}$的这一论断现在被称为Riemann假设．1900年Hilbert把证明或否定Riemann假设列为二十世纪数学家们所面临的最重要的问题之一，但至今此问题仍未解决．

Riemann假设引起许多杰出的数学家的兴趣，而且关于$\zeta(s)$的零点的分布也有大量发现，函方程表明所有的非平凡零点(如果存在的话)必存在于区域$0<\sigma<1$内，即所谓的“临界带”内．容易证明，零点是关于实轴与“临界线”$\sigma=\frac{1}{2}$对称的．

1915年Hardy证明，有无穷多个零点位于临界线上．1921年Hardy与Littlewood证明，如果T充分大，则连结$\frac{1}{2}$与$\frac{1}{2+iT}$的线段上零点的个数至少为AT，A是一个正的常数．1942年，Selberg通过证明该数至少是ATlogT而改进了这一结果，这里A>0．我们知道，当$0<t<T$，$T\to\infty$时，临界带内的零点个数趋于$\frac{T\log T}{2\pi}$．因此，Selberg的结果得到临界线上零点的一个正的分数，最近(1974年)Levinson证明这个分数至少为$\frac{7}{10}$，即Selberg定理中的常数A$\geqslant\frac{7}{20\pi}$．

经过Gram，Baeklund，Lehmer，Haselgrove，Rosser，Yohe，Schoenfeld与其他人的大量的计算看出，实轴上的前面三百五十万个零点是在临界线上的．虽然这些计算有助于Reimann假设，但计算也揭示这样的很自然的现象，即不符合Riemann假设的特例也很可能存在．对$\zeta(s)$的大量计算过程感兴趣的读者请看参考文献[17]．

13.10 对除数函数的应用

素数定理有时可用于估计积性数论函数的数量的阶．本节我们利用它去推导出关于$d(n)$的不等式，$d(n)$表示n的约数的个数．

在第三章里，我们证明了$d(n)$的平均阶是$\log n$，当n是素数时，$d(n)=2$．当n有很多约数时，$d(n)$显然增大．假设n是所有$\leqslant x$的素数的乘积，

即 (28) $n=2\cdot3\cdot5\cdots\cdots p_{\pi(x)}$,

因为$d(n)$是积性的，所以有

$$d(n)=d(2)d(3)\cdots d(p_{\pi(x)})=2^{\pi(x)}.$$

对于大的x，$\pi(x)$近似于$\frac{x}{\log x}$，由(28)得出

$$\log n=\sum_{p\leqslant x}\log p=\vartheta(x)\sim x,$$

所以$2^{\pi(x)}$近似于$2^{\frac{\log n}{\log\log n}}$，于是

$$2^{a\log n}=e^{a\log n\log 2}=n^{a\log 2},$$

$$2^{\frac{\log n}{\log\log n}}=n^{\frac{\log 2}{\log\log n}}.$$

换言之，当n有形式(28)时，$d(n)$近似于$2^{\frac{\log n}{\log\log n}}$
$=n^{\frac{\log 2}{\log\log n}}$.

根据这个想法作下去并稍加细心，我们可得下面关于$d(n)$的不等式.

定理13.12 给定$\varepsilon>0$，则有

(a) 存在一个整数$N(\varepsilon)$，使得$n\geqslant N(\varepsilon)$推出

$$d(n)<2^{\frac{(1+\varepsilon)\log n}{\log\log n}}=n^{\frac{(1+\varepsilon)\log 2}{\log\log n}}.$$

(b) 对无穷多个n，我们有

$$d(n)>2^{\frac{(1+\varepsilon)\log n}{\log\log n}}=n^{\frac{(1-\varepsilon)\log 2}{\log\log n}}.$$

注：这两个不等式等价于关系式

$$\limsup_{n\to\infty}\frac{\log d(n)\log\log n}{\log n}=\log 2.$$

证明 写$n=p_1^{a_1}\cdots p_k^{a_k}$，所以$d(n)=\prod_{i=1}^{k}(a_i+1)$. 我们把乘积分为两部分，素因子$<f(n)$的为一部分，素因子$\geqslant f(n)$的为另一部分. 对$f(n)$的详细说明在后面. 于是

$d(n)=p_1(n)p_2(n)$，其中

$$p_1(n)=\prod_{p_i<f(n)}(a_i+1),\quad p_2(n)=\prod_{p_i\geqslant f(n)}(a_i+1).$$

在乘积$p_2(n)$里，我们利用不等式$(a+1)\leqslant 2^a$，得$p_2(n)\leqslant z^{s(n)}$，其中

$$s(n)=\sum_{\substack{i=1\\ p_i\geqslant f(n)}}^{k} a_i \quad ,$$

这样，

$$n=\prod_{i=1}^{k} p_i{}^{a_i}\geqslant\prod_{p_i\geqslant f(n)} p_i{}^{a_i}\geqslant\prod_{p_i\geqslant f(n)} f(n)^{a_i}=f(n)^{s(n)},$$

于是

$$\log n\geqslant s(n)\log f(n),\quad \text{或}s(n)\leqslant\frac{\log n}{\log f(n)}.$$

这给我们

$$(29)\quad p_2(n)\leqslant 2^{\frac{\log n}{\log f(n)}}.$$

为估计$p_1(n)$，我们写

$$p_1(n)=\exp\left\{\sum_{p_i<f(n)}\log(a_i+1)\right\},$$

并证明，如果n充分大，则$\log(a_i+1)<2\log\log n$．实际上，我们有

$$n\geqslant p_i{}^{a_i}\geqslant 2^{a_i},$$

于是

$$\log n\geqslant a_i\log 2\text{或}a_i\leqslant\frac{\log n}{\log 2}.$$

因此，

$$1+a_i\leqslant 1+\frac{\log n}{\log 2}<(\log n)^2,\ \text{若}n\geqslant n_1$$

对某个n_1成立．即$n\geqslant n_1$推出$\log(1+a_i)<\log(\log n)^2$

$=2\log\log n$. 这给出

$$p_1(n)<\exp\left\{2\log\log n\sum_{p_i<f(n)}1\right\}$$

$$\leqslant\exp\left\{2\log\log n\,\pi(f(n))\right\}.$$

利用不等式$\pi(x)<\frac{6x}{\log x}$（参看定理4.6），得

$$(30)\quad p_1(n)<\exp\left\{\frac{12f(n)\log\log n}{\log f(n)}\right\}$$

$$=2^{cf(n)\frac{\log\log n}{\log f(n)}},$$

其中$c=\frac{12}{\log 2}$，结合(29)与(30)，我们得$d(n)=p_1(n)p_2(n)<2^{g(n)}$，其中

$$g(n)=\frac{\log n+cf(n)\log\log n}{\log f(n)}$$

$$=\frac{\log n}{\log\log n}\,\frac{1+c\frac{f(n)\log\log n}{\log n}}{\frac{\log f(n)}{\log\log n}}.$$

现在我们选取$f(n)$，使$\frac{f(n)\log\log n}{\log n}\to 0$也使$\frac{\log f(n)}{\log\log n}\to 1$当$n\to\infty$时．为此，取

$$f(n)=\frac{\log n}{(\log\log n)^2}$$

即可．于是

$$g(n)=\frac{\log n}{\log\log n}\,\frac{1+o(1)}{1+o(1)}$$

$$=\frac{\log n}{\log\log n}(1+o(1))<(1+\varepsilon)\frac{\log n}{\log\log n}$$

对某个$N(\varepsilon)$成立，当$n\geqslant N(\varepsilon)$时．这证明了(a)．

为证明(b)，我们选取有很多素因子的整数n．实际上，我们取n为$\leqslant x$的所有素数之积，那么，当且仅当$x\to\infty$时，$n\to\infty$．根据素数定理，对这样的n，我们有

$$d(n)=2^{\pi(x)}=2^{\frac{(1+0(1))x}{\log x}},$$

$$\log n=\sum_{p\leqslant x}\log p=g(x)=x(1+0(1)),$$

所以

$$x=\frac{\log n}{1+0(1)}(1+0(1))\log n,$$

于是

$$\begin{aligned}\log x&=\log\log n+\log(1+0(1))\\&=\log\log n\left(1+\frac{\log(1+0(1))}{\log\log n}\right)\\&=(1+0(1))\log\log n.\end{aligned}$$

因此，$\dfrac{x}{\log x}=\dfrac{(1+0(1))\log n}{\log\log n}$且

$$d(n)=2^{\frac{(1+0(1))\log n}{\log\log n}}.$$

对这样的n成立，但对某个$N(\varepsilon)$，如果$n\geqslant N(\varepsilon)$，则有$1+0(1)>1-\varepsilon$，这就证明了(b)． □

注：同定理13.12一样，我们有

$$(31)\quad d(n)=0(n^{\delta})$$

对每个$\delta>0$成立．此结果可以不用素数定理而获得．（参看习题13.13．）

13.11 对Euler函数的应用

上一节所用的理由同样也可用去得到$\varphi(n)$的不等式. 当n是素数时，我们有$\varphi(n)=n-1$，当n有多个素因子时，$\varphi(n)$将更小些. 实际上，如果n是$\leqslant x$的所有素数之积时，我们有

$$\varphi(n)=n\prod_{p\leqslant x}\left(1-\frac{1}{p}\right).$$

下面的定理给出，对于大的x，这个乘积的渐近情况.

定理13.13 对$x\geqslant 2$，有一个正的常数c，使得

$$(32)\quad \prod_{p\leqslant x}\left(1-\frac{1}{p}\right)=\frac{c}{\log x}+O\left(\frac{1}{\log^2 x}\right).$$

注：能证明$c=e^{-C}$. 这里C是Euler常数.（参看[31].）

证明 令$P(x)$表示(32)里的乘积，则$\log P(x)=\sum_{p\leqslant x}\log\left(1-\frac{1}{p}\right)$. 为估计这个和，我们利用幂级数展开式

$$-\log(1-t)=t+\frac{t^2}{2}+\frac{t^3}{3}+\cdots+\frac{t^n}{n}+\cdots \qquad (|t|<1),$$

令$t=\frac{1}{p}$，$a_p=-\log\left(1-\frac{1}{p}\right)-\frac{1}{p}$，移项，得

$$0<a_p=\frac{1}{2p^2}+\frac{1}{3p^3}+\cdots<\frac{1}{2}\left(\frac{1}{p^2}+\frac{1}{p^3}+\cdots\right)=\frac{1}{2p(p-1)}.$$

这表明无穷级数

$$(33)\quad \sum_p a_p=\sum_p\left\{-\log\left(1-\frac{1}{p}\right)-\frac{1}{p}\right\}$$

收敛，因为它不超过$\sum_{n=2}^{\infty}\frac{1}{n(n-1)}$. 如果B表示(33)里的和，则有

$$0<B-\sum_{p\leq x}a_p=\sum_{p>x}a_p<\sum_{n>x}\frac{1}{n(n-1)}$$

$$=-\sum_{n>x}\left(\frac{1}{n}-\frac{1}{n-1}\right)=0\left(\frac{1}{x}\right),$$

于是

$$\sum_{p\leq x}a_p=B+0\left(\frac{1}{x}\right)$$

或

$$-\log p(x)=\sum_{p\leq x}\frac{1}{p}+B+0\left(\frac{1}{x}\right).$$

但据定理4.12，右边的和式是$\log\log x+A+0\left(\frac{1}{\log x}\right)$，所以

$$\log p(x)=-\log\log x-B-A+0\left(\frac{1}{\log x}\right).$$

因此，

$$P(x)=\exp\left\{\log p(x)\right\}$$

$$=e^{-B-A}e^{-\log\log x}e^{0\left(\frac{1}{\log x}\right)}.$$

现在令$c=e^{-B-A}$并利用不等式$e^u=1+0(u)$对$0<u<1$，得

$$p(x)=\frac{c}{\log x}\left\{1+0\left(\frac{1}{\log x}\right)\right\}$$

$$=\frac{c}{\log x}+0\left(\frac{1}{\log^2 x}\right).$$

证明完成.

定理13.14　令c是定理13.13里的常数并令$\varepsilon>0$是给定

的，则有

(a) 存在一个$N(\varepsilon)$，使得

$$\varphi(n)\geqslant(1-\varepsilon)\frac{cn}{\log\log n}\quad 对所有的n\geqslant N(\varepsilon).$$

(b) 对无穷多个n，有

$$\varphi(n)\leqslant(1+\varepsilon)\frac{cn}{\log\log n}.$$

换言之，

$$\liminf_{n\to\infty}\frac{\varphi(n)\log\log n}{n}=c.$$

证明　我们先证明(b)．取$n=\prod_{p\leqslant x}p$，则有

$$\frac{\varphi(n)}{n}=\prod_{p\leqslant x}\left(1-\frac{1}{p}\right)=\frac{c}{\log x}+O\left(\frac{1}{\log^2 x}\right)$$

但$\log n=g(x)=(1+O(1))x$，所以$\log\log n=(1+O(1))\log x$．于是

$$\frac{\varphi(n)}{n}=\frac{c(1+O(1))}{\log\log n}+O\left(\frac{1}{(\log\log n)^2}\right)$$

$$=\frac{c(1+O(1))}{\log\log n}\leqslant(1+\varepsilon)\frac{c}{\log\log n}$$

对某个$N(\varepsilon)$成立，如果$n\geqslant N(\varepsilon)$．这证明了(b)．

为证明(a)，任取$n>1$并写

$$\frac{\varphi(n)}{n}=\prod_{p\mid n}\left(1-\frac{1}{p}\right)=p_1(n)p_2(n),$$

这里，

$$p_1(n)=\prod_{\substack{p\mid n\\ p\leqslant\log n}}\left(1-\frac{1}{p}\right),$$

$$p_2(n)=\prod_{\substack{p\mid n\\ p>\log n}}\left(1-\frac{1}{p}\right).$$

则有

$$(34)\quad p_2(n) > \prod_{\substack{p|n\\ p>\log n}}\left(1-\frac{1}{\log n}\right)=\left(1-\frac{1}{\log n}\right)^{f(n)},$$

其中f(n)是整除n并大于logn的素数的个数．因为

$$n \geqslant \prod_{p|n} p > \prod_{\substack{p|n\\ p>\log n}} p \geqslant (\log n)^{f(n)},$$

我们得到$\log n > f(n)\log\log n$，所以$f(n) < \frac{\log n}{\log\log n}$．因为$1-\left(\frac{1}{\log n}\right)<1$，不等式(34)给我们

$$(35)\quad P_2(n) > \left(1-\frac{1}{\log n}\right)^{\frac{\log n}{\log\log n}}$$

$$=\left\{\left(1-\frac{1}{\log n}\right)^{\log n}\right\}^{\frac{1}{\log\log n}}.$$

而当$u\to\infty$时，$\left(1-\frac{1}{u}\right)^u \to e^{-1}$，所以，当$n\to\infty$时，(35)里最后一部分趋于1．于是(35)给我们

$$p_2(n) > 1+0(1) \quad 当n\to\infty时.$$

因此，

$$\frac{\varphi(n)}{n} = p_1(n)p_2(n) > (1+0(1)) \prod_{\substack{p|n\\ p\leqslant\log n}}\left(1-\frac{1}{p}\right)$$

$$\geqslant (1+0(1)) \prod_{p\leqslant\log n}\left(1-\frac{1}{p}\right)$$

$$=(1+0(1))\frac{c}{\log\log n}(1+0(1))$$

$$\geqslant (1-\varepsilon)\frac{c}{\log\log n}$$

当$n\geqslant N(\varepsilon)$时．这证明了(a)． □

13.12 特征和的Pólya不等式的推广

我们以任一非主特征的Pólya不等式（定理8.21）的推广来结束这一章. 我们利用(31)里得到的除数函数的估计式

$$d(n)=O(n^{\delta})$$

来完成证明.

定理13.15 如果χ是模k的任一非主特征，那么对所有的$x\geqslant 2$，我们有

$$\sum_{m\leqslant x}\chi(m)=O(\sqrt{k}\log k).$$

证明 如果χ是本原的，则由定理8.21得出

$$\sum_{m<x}\chi(m)<\sqrt{k}\log k.$$

现在讨论模k的任一非主特征χ，令c表示χ的前导子，则有$c|k$，$c<k$，并写

$$\chi(m)=\psi(m)\chi_1(m),$$

其中χ_1是模k的主特征而ψ是模c的本原特征. 则有

$$\sum_{m\leqslant x}\chi(m)=\sum_{\substack{m\leqslant x\\(m,k)=1}}\psi(m)=\sum_{m\leqslant x}\psi(m)\sum_{d|(m,k)}\mu(d)$$

$$=\sum_{m\leqslant x}\sum_{\substack{d|k\\d|m}}\mu(d)\psi(m)=\sum_{d|k}\mu(d)\sum_{q<\frac{x}{d}}\psi(qd)$$

$$=\sum_{d|k}\mu(d)\psi(d)\sum_{q<\frac{x}{d}}\psi(q).$$

于是有

$$\left|\sum_{m<x}\chi(m)\right|\leqslant\sum_{d|k}|\mu(d)\psi(d)|\left|\sum_{q<\frac{x}{d}}\psi(q)\right| \tag{36}$$

$$<\sqrt{c}\log c\sum_{d|k}|\mu(d)\psi(d)|,$$

这因为ψ是模c的本原特征．在最后的和式里，每一个因子$|\mu(d)\psi(d)|$为0或1．如果$|\mu(d)\psi(d)|=1$，则$|\mu(d)|=1$，所以d是k的非平方因子，即

$$d=p_1p_2\cdots p_r.$$

还有$|\psi(d)|=1$，所以$(d,c)=1$，就是说，没有一个素因子p_i能整除c，于是每一个p_i整除$\frac{k}{c}$，所以d整除$\frac{k}{c}$，换言之，

$$\sum_{d\mid n}|\mu(d)\psi(d)|\leqslant\sum_{d\mid\frac{k}{c}}1=d\left(\frac{k}{c}\right)=0\left(\left(\frac{k}{c}\right)^{\delta}\right)$$

对任一$\delta>0$成立．特别，$d\left(\frac{k}{c}\right)=0\left(\sqrt{\frac{k}{c}}\right)$，所以(36)推出

$$\sum_{m\leqslant x}\chi(m)=0\left(\sqrt{\frac{k}{c}}\sqrt{c}\log c\right)=0(\sqrt{k}\log c)$$
$$=0(\sqrt{k}\log k).$$

□

第十三章习题

1. Chebyshev证明，当$x\to\infty$时，如果$\frac{\psi(x)}{x}$趋于一个极限，则此极限等于1．在习题4.26里有一个证明的概要．本题给出另一个证明的纲要，它以习题11.1(d)给出的等式

$$(37)\quad -\frac{\zeta'(s)}{\zeta(s)}=s\int_1^{\infty}\frac{\psi(x)}{x^{s+1}}dx\quad(\sigma>1)$$

为基础．

(a) 证明 $\frac{(1-s)\zeta'(s)}{\zeta(s)}\to1$ 当$s\to1$时．

(b) 令$\delta=\limsup\limits_{x\to\infty}\left(\frac{\psi(x)}{x}\right)$,给定$\varepsilon>0$,选取$N=N(\varepsilon)$,使$x\geqslant N$推出$\psi(x)\leqslant(\delta+\varepsilon)x$. 保持s为实数且$1<s\leqslant2$,将(37)里的积分分为两部分:$\int_1^N+\int_N^\infty$,估计每一部分,得不等式

$$-\frac{\zeta'(s)}{\zeta(s)}\leqslant C(\varepsilon)+\frac{s(\delta+\varepsilon)}{s-1},$$

其中$C(\varepsilon)$是一个不依赖于s的常数. 利用(a)推出$\delta\geqslant1$.

(c) $r=\liminf\limits_{x\to\infty}\left(\frac{\psi(x)}{x}\right)$,利用类似的理由推出$r\leqslant1$.因此,当$x\to\infty$时,如果$\frac{\psi(x)}{x}$趋于一个极限,则$r=\delta=1$.

2. 令$A(x)=\sum_{n\leqslant x}a(n)$,其中

$$a(n)=\begin{cases}0 & \text{如果}n\neq\text{一个素数的方幂},\\ \frac{1}{k} & \text{如果}n=P^k.\end{cases}$$

证明,$A(x)=\pi(x)+O(\sqrt{x}\log\log x)$.

3. (a) 如果$c>1$并且$x\neq$整数,证明,当$x>1$时,有

$$\frac{1}{2\pi i}\int_{c-\infty i}^{c+\infty i}\log\zeta(s)\frac{x^s}{s}ds$$

$$=\pi(x)+\frac{1}{2}\pi(x^{\frac{1}{2}})+\frac{1}{3}\pi(x^{\frac{1}{3}})+\cdots.$$

(b) 素数定理等价于渐近关系式

$$\frac{1}{2\pi i}\int_{c-\infty i}^{c+\infty i}\log\zeta(s)\frac{x^s}{s}ds\sim\frac{x}{\log x}\quad\text{当}x\to\infty\text{时}.$$

素数定理的一个证明就是基于这个关系式由Landau在1903年给出的.

4. 令$M(x)=\sum_{n\leqslant x}\mu(n)$. 对于大的x,M(x)的数量的确切

的阶还不知道．在第四章里证明了，素数定理等价于关系式$M(x)=o(x)$，当$x\to\infty$时．本题把$M(x)$的数量的阶与Riemann假设联系起来．

设有一个正的常数Q，使得

$$M(x)=O(x^Q) \quad 对x\geqslant 1.$$

证明对$\sigma>1$成立的公式（参看习题11.1(c)）

$$\frac{1}{\zeta(s)}=s\int_1^{\infty}\frac{M(x)}{x^{s+1}}dx$$

对$\sigma>Q$也成立．对$\sigma>Q$，推导出$\zeta(s)\neq 0$．特别，这说明关系式$M(x)=O(x^{\frac{1}{2}+\varepsilon})$对每一个$\varepsilon>0$成立能推出Riemann假设．它也说明，由Riemann假设能推出$M(x)=O(x^{\frac{1}{2}+\varepsilon})$对每一个$\varepsilon>0$成立．（参看Titchmarsh[69]，P.315.）

5．证明下面的引理，它类似于引理2．令

$$A_1(x)=\int_1^x\frac{A(u)}{u}du,$$

其中$A(u)$是一个对$u\geqslant 1$非负递增的函数．如果我们有渐近式

$$A_1(x)\sim Lx^c \quad 当x\to\infty时$$

对某个$c>0$与$L>0$，那么我们也有

$$A(x)\sim cLx^c \quad 当x\to\infty时.$$

6．证明

$$\frac{1}{2\pi i}\int_{2-\infty i}^{2+\infty i}\frac{y^s}{s^2}ds=0 \quad 若0<y<1.$$

如果$y\geqslant 1$，这个积分的值是什么？

7．把

$$\frac{1}{2\pi i}\int_{2-\infty i}^{2+\infty i}\frac{x^s}{s^2}\left(-\frac{\zeta'(s)}{\zeta(s)}\right)ds$$

表示为含有$\Lambda(n)$的有限和.

8. 令χ是模k的任一Dirichlet特征，而χ_1是主特征，定义

$$F(\sigma,t)=3\frac{L'}{L}(\sigma,\chi_1)+4\frac{L'}{L}(\sigma+it,\chi)$$
$$+\frac{L'}{L}(\sigma+2it,\chi^2),$$

如果$\sigma>1$，证明$F(\sigma,t)$的实部等于

$$-\sum_{n=1}^{\infty}\frac{\Lambda(n)}{n^{\sigma}}R_e\{3\chi_1(n)+4\chi(n)n^{-it}$$
$$+\chi^2(n)^{-2it}\},$$

并推导出$R_e F(\sigma,t)\leqslant 0$.

9. 假设$L(s,\chi)$在$s=1+it$有阶数为$m\geqslant 1$的零点，证明，对这个t，我们有

(a) $\frac{L'}{L}(\sigma+it,\chi)=\frac{m}{\sigma-1}+0(1)$ 当$\sigma\to 1_+$时.

(b) 存在一个整数$r\geqslant 0$，使得

$$\frac{L'}{L}(\sigma+2it,\chi^2)=\frac{r}{\sigma-1}+0(1)\quad 当\sigma\to 1_+ 时.$$

除开$\chi^2=\chi_1$与$t=0$之外都成立.

10. 利用8,9题，证明

如果$\chi^2\neq\chi_1$，则$L(1+it,\chi)\neq 0$对所有的实数t.

如果$\chi^2=\chi_1$，则$L(1+it,\chi)\neq 0$对所有的实数$t\neq 0$.

[提示：讨论$F(\sigma,t)$，当$\sigma\to 1_+$时.]

11. 对任一数论函数$f(n)$，证明下列论断等价：

(a) $f(n)=0(n^{\varepsilon})$对每一个$\varepsilon>0$与所有的$n\geqslant n_1$.

(b) $f(n)=0(n^{\delta})$对每一个$\delta>0$当$n\to\infty$时.

12. 令$f(n)$是一个积性函数，使得，若p是素数，有

$$f(p^m)\to 0 \quad 当p\to\infty时.$$

即，对每一个$\varepsilon>0$，存在一个$N(\varepsilon)$,使得,当$p^m>N(\varepsilon)$时，有$|f(p^m)|<\varepsilon$. 由此证明，当$n\to\infty$时，$f(n)\to 0$.
[提示：存在一个常数$A>0$，使得$|f(p^m)|<A$对所有的素数p与所有的$m\geqslant 0$成立. 并且存在一个常数$B>0$，使得当$p^m>B$时，有$|f(p^m)|<1$.]

13. 如果$\alpha\geqslant 0$，则令$\sigma_\alpha(n)=\sum_{d\mid n}d^\alpha$,证明，对每一个$\delta>0$，我们有

$$\sigma_\alpha(n)=O(n^{\alpha+\delta}) \quad 当n\to\infty时.$$

[提示：利用12题.]

第十四章　分　拆

14.1　引言

迄今，本书只讨论了乘法数论，它研究关于整数的素因子分解的数论函数．现在我们转向数论的另一个分枝—加法数论，其中一个基本问题是把一个给定的正整数n表示为一个给定的集合A中整数的和，比如

$$A=\{a_1,a_2,\cdots\},$$

其中元素a_i是一些特殊的数，如素数，平方数，立方数，三角形数等等．把n表示为A中元素之和的每一种表示法称为n的一个分拆．我们的兴趣在于数论函数$A(n)$，它计算在A中取加数作n的分拆的个数．我们用一些著名的例子来说明．

Goldbach猜想　每一个偶数$n>4$是两个奇素数的和．

在这个例子里，$A(n)$是方程

(1)　$n=p_1+p_2$

的解的个数．其中p_i是奇素数．Goldbach判断是，对每一个偶数$n>4$，$A(n)\geqslant 1$．这个猜想于1742年提出，至今仍未解决．1973年，苏联数学家Vinogradov证明，每一个充分大的奇数是三个奇素数之和．1966年，中国数学家陈景润证明，每一个充分大的偶数是一个奇素数一个奇因子不超过

两个的数之和．（参考文献[10]．）

平方表示　对一个给定的整数$k\geq 2$，考虑分拆函数$r_k(n)$，这个函数是计算方程

（2）$n=x_1^2+x_2^2+\cdots+x_k^2$

的解的个数，其中x_i可以是正的、负的或是0，加数的顺序也考虑在内．

对于$k=2$，4，6，8，Jacobi[34]用除数函数来表示$r_k(n)$．例如，他证明

$$r_2(n)=4\{d_1(n)-d_3(n)\},$$

其中$d_1(n)$与$d_3(n)$分别是与1，3同余mod4的n的约数的个数．比如，$r_2(5)=8$，这因为5的两个约数1与5对模4都同余于1．实际上，由

$$5=2^2+1^2=(-2)^2+1^2=(2)^2+(-1)^2$$
$$=2^2+(-1)^2$$

给出4种表示法且交换加数的顺序还有4种表示法．

对于$k=4$，Jacobi证明

$$r_4(n)=\sum_{d\mid n}d=8\sigma(n)\quad 若n为奇数$$
$$=24\sum_{\substack{d\mid n\\ d为奇数}}d\quad 若n为偶数.$$

$r_6(n)$与$r_8(n)$的公式更复杂些但是同样普通类型．（参看[14]．）

对于$k=3$，5，7也有准确公式，它们包含有二次剩余的Legendre符号的推广—Jacobi符号．例如，当n是奇素数时，知道

$$r_3(n)=24\sum_{m<\frac{n}{4}}\left(\frac{m}{n}\right)\quad 若n\equiv 1(\mathrm{mod}4)$$

$$=8\sum_{m\leqslant\frac{n}{2}}\left(\frac{m}{n}\right)\quad 若n\equiv 3(\mathrm{mod}4).$$

(2)里的数x_1, x_2, x_3在这里是互素的.

对于大的值k，分拆$r_k(n)$更复杂得多. 有一个关于这个问题的巨大的文献是由Mordell，Hardy，Littlewood，Ramanujan以及其他很多人作出的贡献. 对于$k\geqslant 5$，知道$r_k(n)$能由形如

(3) $r_k(n)=p_k(n)+R_k(n)$

的渐近公式表示. 其中$p_k(n)$是主项，由无穷级数

$$p_k(n)=\frac{\pi^{\frac{k}{2}}n^{\frac{k}{2}-1}}{\Gamma\left(\frac{k}{2}\right)}\sum_{q=1}^{\infty}\sum_{\substack{h=1\\(h,q)=1}}^{p}\left(\frac{G(h;q)}{q}\right)^k e^{\frac{-2\pi i n h}{q}}$$

给定，而$R_k(n)$是较小的阶的阶的余项. $p_k(n)$称为奇异级数而$G(h;q)$是二次Gauss和，

$$G(h;q)=\sum_{r=1}^{q}e^{\frac{2\pi i r^2}{q}}.$$

1917年，Mordell注意到$r_k(n)$是级数

$$g=1+2\sum_{n=1}^{\infty}x^{n^2}$$

的k次方的幂级数表示式里的x^n的系数.函数g与椭圆模函数有关，它在(3)式的推导过程中起着重要作用.

Waring问题　对一个给定的正整数k，确定是否有一个整数s，(仅依赖于k，)使得方程

(4) $n=x_1^k+x_2^k+\cdots+x_s^k$

对每一个$n\geqslant 1$有解.

这个问题的名字是英国数学家E.Waring，他在1770年

推断（没有证明而有有限个数的证据），每一个n是4个平方数的和，9个立方数的和，19个4次方幂的和等等. 在这个例子里，分拆函数$A(n)$是(4)的解的个数，并且这个问题是确定是否存在一个s，使得对所有的n，$A(n)\geq 1$.

对一个整数k，如果s存在，那么有一个s的最小值，把它记为$g(k)$. Lagrange在1770年证明了$g(2)$的存在性，在其后的139年里，对$k=3$，4，5，6，7，8与10，知道了$g(k)$的存在性. 1909年Hilbert对k用归纳法，证明了$g(k)$的存在性，但对任何一个k，没有确定$g(k)$的数字. 现在，除了$k=4$以外，对每一个k，$g(k)$的确切的值是知道的. Hardy与Littlewood给出(4)的解数的渐近公式，这个公式用类似于(3)里的奇异级数来表示. 关于Waring问题的历史叙述请看W.J.Ellison[18].

自由分拆　在加法数论里，最基本的问题之一是自由分拆. 在这里，加数的集合由所有的正整数组成，而所研究的分拆函数是n能写为$\leq n$的正整数之和的方法数，即

$$(5)\quad n=a_{i_1}+a_{i_2}+\cdots$$

的解的个数，这里加数的个数是自由的，允许相同而加数的顺序不计. 对应的分拆函数用$p(n)$表示并称为自由分拆函数，或简称为分拆函数. 加数称为部分. 例如，4的分拆恰有5个，

$$4=3+1=2+2=2+1+1=1+1+1+1,$$

所以$p(4)=5$. 类似地，$p(5)=7$，5的分拆是

$$5=4+1=3+2=3+1+1=2+2+1=2+1+1+1$$
$$=1+1+1+1+1.$$

本章余下部分专门研究$p(n)$与有关函数.

14.2 分拆的几何表示

分拆有一个简单的几何表示的方法，它利用称为网络的格点表示出来．例如15的一个分拆为

$$6+3+3+2+1,$$

它能由15个格点排成5行表示如下：

```
· · · · · ·
· · ·
· · ·
· ·
·
```

如果我们垂直地读这个网络，我们得到15的另一个分拆

$$5+4+3+1+1+1,$$

两个这样的分拆称为是共轭的．注意，这两个分拆中的任一个的最大部分等于另一个分拆的部分的个数．我们有下面的定理．

定理14.1　n分为m个部分的分拆的个数等于n的最大部分为m的分拆的个数．

几个定理能用简单的包含网络的组合理由给予证明．我们将回到这个方法的上面的美妙图解．此外，分拆理论里最深奥的结果需要更多的解析理论，现在我们转向它．

14.3 分拆的生成函数

由Dirichlet级数$F(s)=\sum f(n)n^{-s}$定义的函数$F(s)$称

为系数$f(n)$的生成函数．在乘法数论里，Dirichlet级数是常用的生成函数，因为$n^{-s}m^{-s}=(nm)^{-s}$．在加法数论里，利用幂级数$F(x)=\sum f(n)x^n$表示的生成函数更方便，因为$x^n x^m=x^{n+m}$．下面的定理给出分拆函数$p(n)$的一个生成函数．

定理14.2 Euler．对$|x|<1$，我们有

$$\prod_{m=1}^{\infty}\frac{1}{1-x^m}=\sum_{n=0}^{\infty}p(n)x^n,$$

其中$p(0)=1$．

证明 我们先给出产生这个等式的公式，而不管它的收敛性，然后才给出更严格的证明．

如果乘积里的每一个因子展开为一个幂级数（几何级数），我们得

$$\prod_{m=1}^{\infty}\frac{1}{1-x^m}=(1+x+x^2+\cdots)(1+x^2+x^4+\cdots)$$
$$(1+x^3+x^6+\cdots)\cdots,$$

右边这些级数相乘时，把它们看作多项式，并把x的同次方幂集中在一起，得到如下的一个幂级数

$$1+\sum_{k=1}^{\infty}a(k)x^k,$$

我们将证明$a(k)=p(k)$．假如我们从第一个级数中取项x^{k_1}，第二个级数中取项x^{2k_2}，第三个级数中取项x^{3k_3}，…，第m个级数中取项x^{mk_m}，其中每个$k_i\geqslant 0$，则其乘积是

$$x^{k_1}x^{2k_2}x^{3k_3}\cdots x^{mk_m}=x^k$$

所以

$$k=k_1+2k_2+3k_3+mk_m.$$

这也能写为下面的式子：

$$k=(1+1+\cdots+1)+(2+2+\cdots+2)+\cdots+(m+m+\cdots+m),$$

其中第一个括号里含有k_1个1，第二个括号里含有k_2个2，等等，这正好是将k分为正整数之和的一个分拆，即k的每一个分拆产生这样一项x^k. 反之，每一项x^k来自k的一个相应的分拆. 因此x^k的系数$a(k)$等于k的分拆的个数$p(k)$.

上述理由不是一个严格的证明，因为我们没有考虑收敛性，而把无限多个几何级数看作多项式乘在一起. 但是，把上面的想法改变为一个严格的证明是不难的.

为此目的，我们限制x在区间$0\leqslant x<1$内，并引入两个函数

$$F_m(x)=\prod_{k=1}^{m}\frac{1}{1-x^k},$$

$$F(x)=\sum_{k=1}^{\infty}\frac{1}{1-x^k}=\lim_{m\to\infty}F_m(x).$$

定义的乘积$F(x)$在$0\leqslant x<1$内绝对收敛，因为它的倒数$\Pi(1-x^k)$绝对收敛（因为级数$\sum x^k$绝对收敛）. 还要注意，对每一个固定的x，序列$\{F_m(x)\}$是递增的，因为

$$F_{m+1}(x)=\frac{1}{1-x^{m+1}}F_m(x)\geqslant F_m(x),$$

即$F_m(x)\leqslant F(x)$对$0\leqslant x<1$内的每一个固定的x与每一个m成立. 于是，$F_m(x)$是有限个绝对收敛的级数的乘积，因此$F_m(x)$也是绝对收敛的级数，我们能写

$$F_m(x)=1+\sum_{k=1}^{\infty}p_m(k)x^k,$$

其中$p_m(k)$是方程

$$k=k_1+2k_2+\cdots+mk_m$$

的解的个数．换言之，$p_m(k)$是把k分为不超过m个部分的分拆的个数．如果$m\geqslant k$，则有$p_m(k)=p(k)$．因此，我们总是有

$$p_m(k)\leqslant p(k),$$

当$m\geqslant K$时，取等号，换言之，我们有

$$\lim_{m\to\infty}p_m(k)=p(k)$$

现在，我们把$F_m(x)$的级数分为两部分，

$$F_m(x)=\sum_{k=0}^{m}p_m(k)x^k+\sum_{k=m+1}^{\infty}p_m(k)x^k$$

$$=\sum_{k=0}^{m}p(k)x^k+\sum_{k=m+1}^{\infty}p_m(k)x^k.$$

因为$x\geqslant 0$，我们有

$$\sum_{k=0}^{m}p(k)x^k\leqslant F_m(x)\leqslant F(x),$$

这说级数$\sum_{k=0}^{\infty}p(k)x^k$收敛．此外，因为$p_m(k)\leqslant p(k)$，所以有

$$\sum_{k=0}^{\infty}p_m(k)x^k\leqslant\sum_{k=0}^{\infty}p(k)x^k\leqslant F(x),$$

故，对每一个固定的x，级数$\sum p_m(k)x^k$在m里一致收敛．令$m\to\infty$，得

$$F(x)=\lim_{m\to\infty}F_m(x)=\lim_{m\to\infty}\sum_{k=0}^{\infty}p_m(k)x^k$$

$$=\sum_{k=0}^{\infty}\lim_{m\to\infty}p_m(k)x^k=\sum_{k=0}^{\infty}p(k)x^k,$$

这证明了Euler等式对$0\leqslant x<1$成立．根据解析开拓，我们能把它扩大到单位圆$|x|<1$内． □

根据类似的理由，我们能容易地得到很多其它的分拆的

表14.1 生 成 函 数

生 成 函 数	n分为部分的分拆数是
$\prod_{m=1}^{\infty}\frac{1}{1-x^{2m-1}}$	奇数
$\prod_{m=1}^{\infty}\frac{1}{1-x^{2m}}$	偶数
$\prod_{m=1}^{\infty}\frac{1}{1-x^{m^2}}$	平方数
$\prod_{p}\frac{1}{1-x^{p}}$	素数
$\prod_{m=1}^{\infty}(1+x^{m})$	不等的数
$\prod_{m=1}^{\infty}(1+x^{2m-1})$	奇数并是不相等的数
$\prod_{m=1}^{\infty}(1+x^{2m})$	偶数且不相等
$\prod_{m=1}^{\infty}(1+x^{m^2})$	不同的平方数
$\prod_{p}(1+x^{p})$	不同的素数

生成函数．我们在表14.1里提到的只是少数几个例子．

14.4 Euler五边形数定理

下面我们讨论生成函数为乘积$\Pi(1-x^m)$的分拆函数．

$\Pi(1-x^m)$是$p(n)$的生成函数的倒数，写为

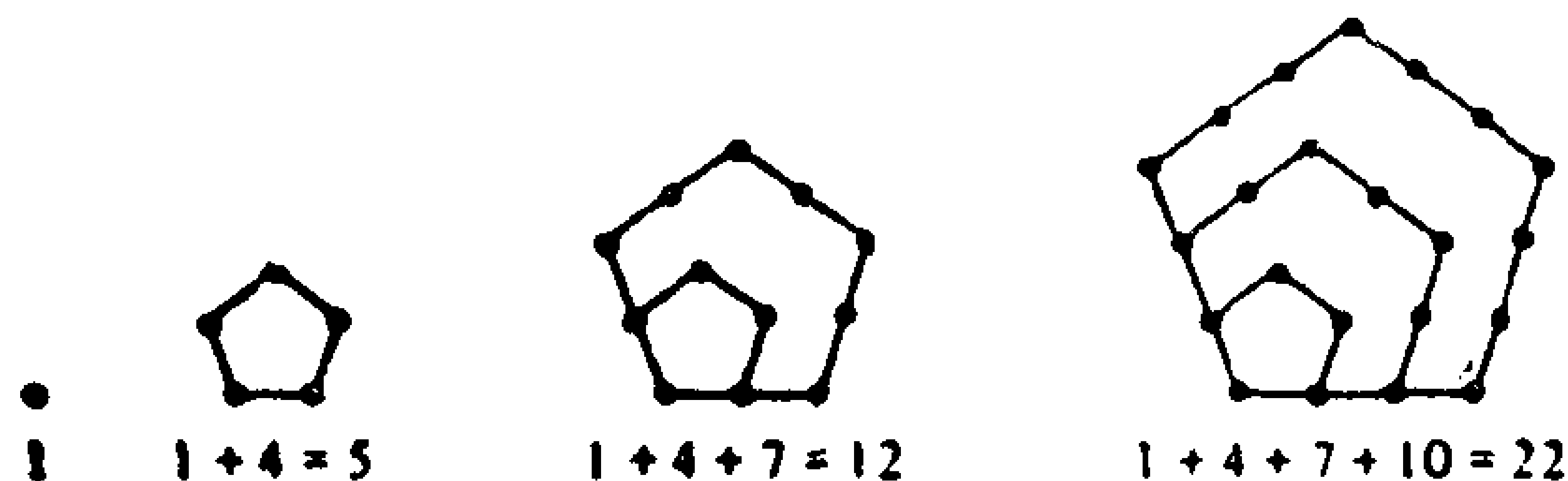
$$\prod_{m=1}^{\infty}(1-x^m)=1+\sum_{n=1}^{\infty}a(n)x^n.$$

为了把$a(n)$表为分拆函数，我们注意，n分为不相等部分的每一个分拆在等式右边都产生一个系数为$+1$或-1的项x^n，若x^n是偶数个项的乘积，则系数是$+1$，若x^n是奇数个项的乘积，则系数为-1。因此

$$a(n)=p_e(n)-p_o(n),$$

其中$p_e(n)$是把n分为偶数个不相等部分的分拆的个数，$p_o(n)$是把n分为奇数个不相等部分的分拆的个数。Euler证明，除开n属于一个称为五边形数的特殊集合之外，对所有其它的n，都有$p_e(n)=p_o(n)$。

五边形数1，5，12，22，…在本书开始的历史介绍中被提到过，它们与五边形的联系如图14.1。



(图14.1)

这些数也是下面的算术级数的部分和，

$$1,\ 4,\ 7,\ 10,\ 13,\ \cdots,\ 3n+1,\ \cdots$$

如果$\omega(n)$表示这个级数的前n项之和，则

$$\omega(n)=\sum_{k=0}^{n-1}(3k+1)=\frac{3n(n-1)}{2}+n$$

$$=\frac{3n^2-n}{2}.$$

数$\omega(n)$与$\omega(-n)=\frac{(3n^2+n)}{2}$称为五边形数.

定理14.3 Euler五边形数定理. 如果$|x|<1$, 则有

$$\prod_{m=1}^{\infty}(1-x^m)=1-x-x^2+x^5+x^7-x^{12}-x^{15}+\cdots$$
$$=1+\sum_{n=1}^{\infty}(-1)^n\{x^{\omega(n)}+x^{\omega(-n)}\}$$
$$=\sum_{n=-\infty}^{\infty}(-1)^n x^{\omega(n)}.$$

证明 我们先证明结果对$0\leqslant x<1$成立并根据解析开拓把它扩大到圆$|x|<1$. 规定$P_0=S_0=1$, 并对$n\geqslant 1$, 令

$$P_n=\prod_{r=1}^{n}(1-x^r),$$

$$S_n=1+\sum_{r=1}^{n}(-1)^r\{x^{\omega(r)}+x^{\omega(-r)}\}.$$

由于无穷乘积$\Pi(1-x^m)$收敛, 所以, 当$x\to\infty$时, $P_n\to\Pi(1-x^m)$. 我们证明(利用Shank方法[63])

(6) $|S_n-P_n|\leqslant nx^{n+1}$.

因为当$n\to\infty$时, $nx^{n+1}\to 0$, 这证明Euler等式对$0\leqslant x<1$成立.

为证明(6), 我们令$g(r)=\frac{r(r+1)}{2}$并引入和式

$$F_n=\sum_{r=0}^{n}(-1)^r\frac{P_n}{P_r}x^{rn+g(r)}.$$

首先, 我们指出, F_n是S_n的变形. 容易验证, $F_1=S_1=1-x-x^2$, 因此, 若能证明

$F_n-F_{n-1}=S_n-S_{n-1}$ 或 $F_n-S_n=F_{n-1}-S_{n-1}$,

这就证明$F_n=S_n$对所有$n\geqslant 1$. 由于

$$F_n - F_{n-1} = \sum_{r=0}^{n}(-1)^r \frac{P_n}{P_r} x^{rn+g(r)} - \sum_{r=0}^{n-1}(-1)^r \frac{P_n}{P_r} x^{r(n-1)+g(r)}$$

在前一个和式里，我们写$P_n=(1-x^n)P_{n-1}$并分离出$r=n$这一项，我们把差$1-x^n$分类，得

$$\begin{aligned}F_n - F_{n-1} = &(-1)^n x^{n^2+g(n)} \\ &+ \sum_{r=0}^{n-1}(-1)^r \frac{P_n}{P_r} x^{rn+g(r)} \\ &- \sum_{r=0}^{n-1}(-1)^r \frac{P_{n-1}}{P_r} x^{(r+1)n+g(r)} \\ &- \sum_{r=0}^{n-1}(-1)^r \frac{P_{n-1}}{P_r} x^{r(n-1)+g(r)}\end{aligned}$$

现在把第一与第三个和式放在一起，并注意消掉$r=0$那一项，在第二个和式里，我们作指标替换，得

$$\begin{aligned}F_n - F_{n-1} = &(-1)^n x^{n^2+g(n)} \\ &+ \sum_{r=1}^{n-1}(-1)^r \frac{P_{n-1}}{P_r} x^{r(n-1)+g(r)}(x^r-1) \\ &- \sum_{r=1}^{n}(-1)^{r-1} \frac{P_{n-1}}{P_{r-1}} x^{rn+g(r-1)}.\end{aligned}$$

但$\dfrac{(x^r-1)}{P_r}=\dfrac{-1}{P_{r-1}}$且$r(n-1)+g(r)=rn+g(r-1)$，所以最后的两个和式除开第二个和式中的$r=n$这一项外，其余各项均可消去，故得

$$F_n - F_{n-1} = (-1)^n x^{n^2+g(n)} + (-1)^n x^{n^2+g(n-1)}.$$

但是

$$n^2+g(n)=n^2+\frac{n(n+1)}{2}=\omega(-n),$$

$$n^2+g(n-1)=\omega(n),$$

所以

$$F_n - F_{n-1} = (-1)^n\{x^{\omega(n)} + x^{\omega(-n)}\} = S_n - S_{n-1},$$

于是，对所有的$n \geqslant 1$，$F_n = S_n$. 定义F_n的和式里的第一项是 P_n，所以，

$$(7)\quad F_n = P_n + \sum_{r=1}^{n}(-1)^r \frac{P_n}{P_r} x^{rn+g(r)},$$

注意，$0 < \frac{P_n}{P_r} \leqslant 1$，因为$0 \leqslant x < 1$. 还有，每一个因子$x^{rn+g(r)} \leqslant x^{n+1}$，所以(7)式右边的和不超过$nx^{n+1}$，因此$|F_n - P_n| \leqslant nx^{n+1}$. 又因$F_n = S_n$. 这证明了(6)并完成了Euler等式的证明. □

14.5 Euler五边形数定理的组合证明

Euler在1750年用归纳法证明了他的五边形数定理. 其后，Legendre在1830年，Jacobi在1846年分别得到证明. 本节叙述叙述F.Franklin[22]在1881年给出的一个著名的组合证明.

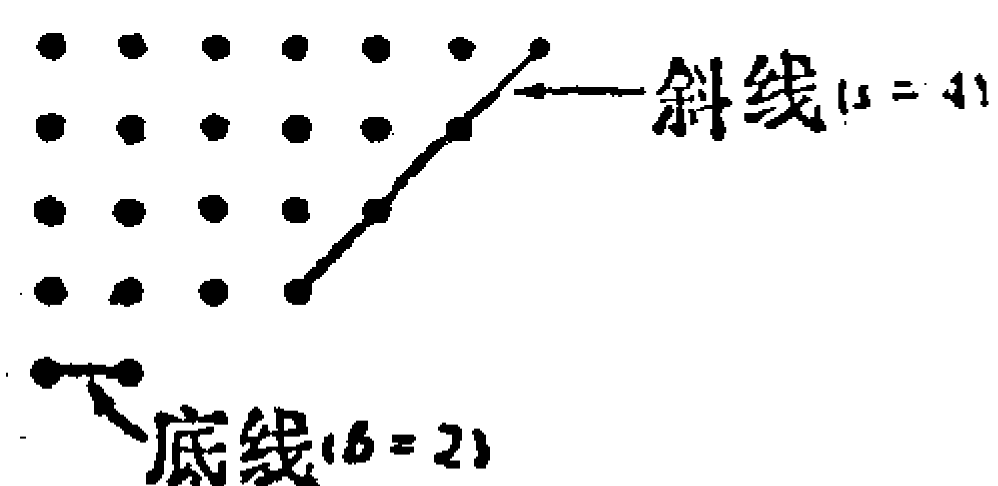
我们知道

$$\prod_{m=1}^{\infty}(1 - x^m) = 1 + \sum_{n=1}^{\infty}\{P_e(n) - P_o(n)\}x^n,$$

其中$P_e(n)$是n分为偶数个不相等部分的分拆的个数，$P_o(n)$是n分为奇数个不相等部分的分拆的个数. Franklin利用分拆的格点图象表示去证明，把n分为偶数个不相等部分与分为奇数个不相等部分的分拆之间有一一对应关系，所以$P_e(n) = P_o(n)$，除开n是一个五边形数之外.

考虑把n分为不相等部分的任一分拆的图象. 如果这些部分是依次递减排列的话，如同以图14.2为例表明的那样，

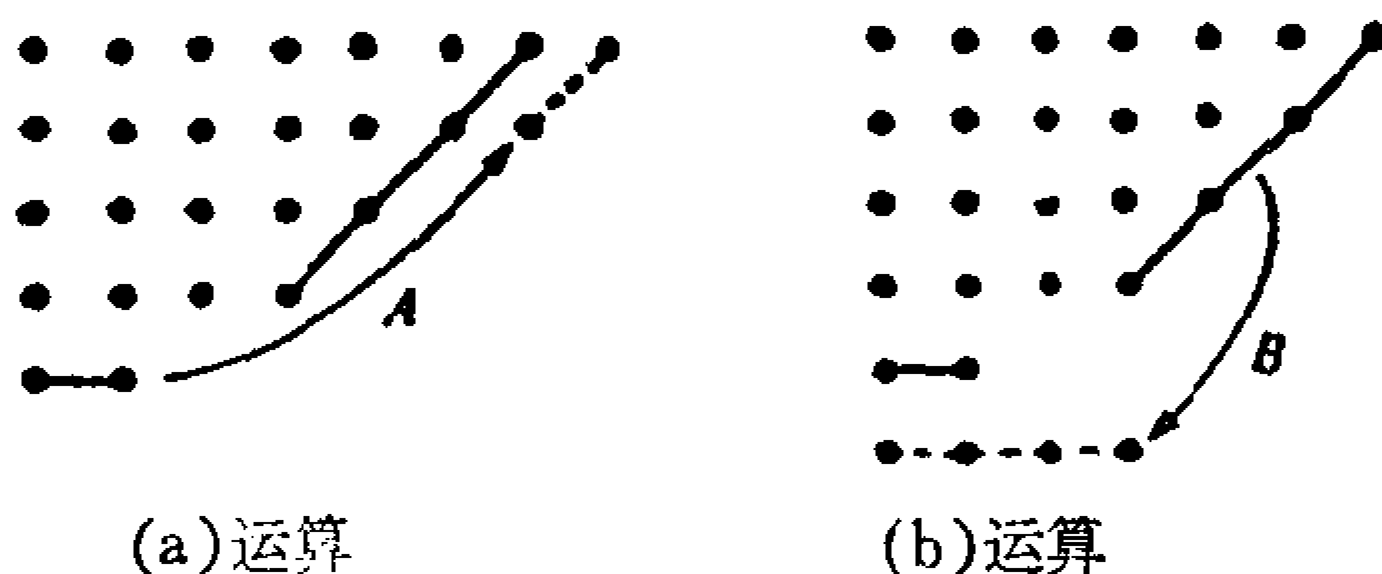
我们就说这个图形是一个标准形式．连结最后一行各点的最长的线段称为这个图形的底线，并把底线上格点的个数记为b，于是b≥1．在图形里，连结第一行与其它各行的最后的点的最长的45°的线段叫做斜线，斜线上格点的个数记为S，于是S≥1．



（图14.2）

在图14.2里，b＝2，s＝4．

现在我们在图上规定两种运算A与B．运算A就是移动底线上各点使它与斜线平行，如图14.3(a)所示．运算B就是移动斜线上的点使它与底线平行，如图14.3(b)所示．我们说一个运算是可允许的，如果它能保持图形的标准形式．即，如果新图形的不相等部分仍然排为递减顺序．



(a)运算　　(b)运算

（图14.3）

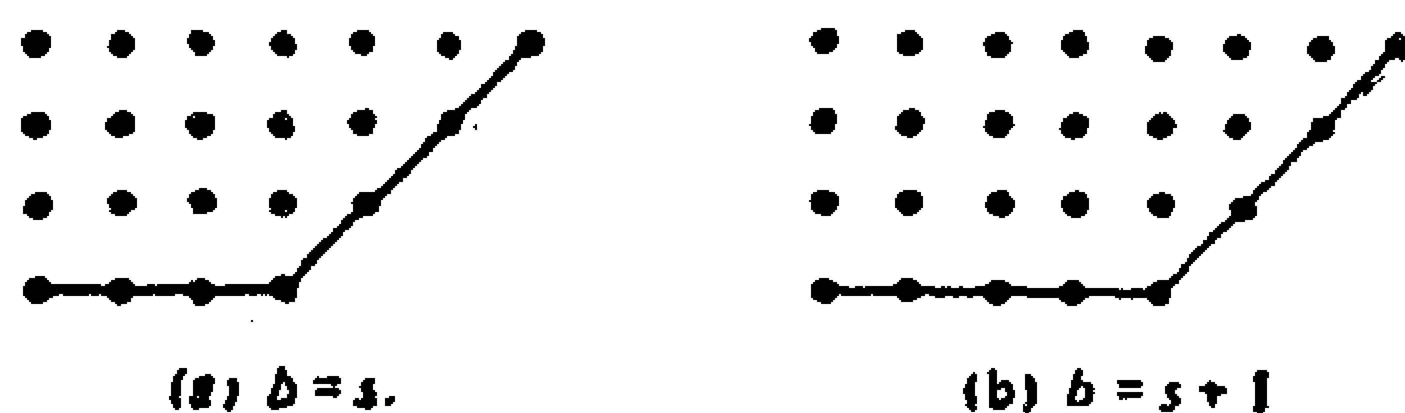
如果A是可允许的，我们就得到把n分为不相等部分的一个新的分拆，但部分的个数比原来减少1个．如果B是可允许的，我们也得到n分为不相等的部分的一个新的分拆，但部分的个数比原来大1．因此，对n的任一分拆，如果A或B确有一个是可允许的，那么n分为奇数个与偶数个不相等部分之间有一个一一对应关系，所以，对这样的n，有$P_e(n)=P_e(n)$．

为确定A或B谁是可允许的，我们讨论三种情形：(1) $b<s$；(2) $b=s$；(3) $b>s$.

情形(1)：若$b<s$，则$b\leqslant s-1$，所以A是可允许但B是不允许的，因为B破坏了标准形式(图14.3).

情形(2) 若$b=s$，则B是不允许的，因为它在新图上的结果不是标准形式．运算A是可允许的，但要除开底线与斜线相交这个例外，因为这时新图不是标准形式．(图14.4(a).)

情形(3) 若$b>s$，则A是不允许的而B是可允许的，除开$b=s+1$且底线与斜线相交这个例外，这时新图包含有两个相等部分．(图14.4(b).)



(图14.4)　A与B都不是可允许的

因此，A或B一定有一个是可允许的，除开上面指出的两个例外．考虑图14.4(a)里指出的第一个例外情形，假定图里有K行，则$b=k$，由

$$n=k+(k+1)+\cdots+(2k-1)=\frac{3k^2-k}{2}=\omega(k)$$

给定n．对于n的这个分拆，如果k是偶数，我们就有n分为偶数个部分的一个特殊分拆，如果k是奇数，我们就有n分为奇数个部分的一个特殊分拆．所以

$$P_e(n)-P_o(n)=(-1)^k.$$

图14.4(b)里指出的另一个例外的情形里，每一行增加一个格点，所以

$$n=\frac{3k^2-k}{2}+k=\frac{3k^2+k}{2}=\omega(-k),$$

仍然有$P_e(n)=P_o(n)=(-1)^k$. Franklin证明完成 □

14.6 P(n)的Euler递推公式

定理14.4 令$P(0)=1$并规定当$n<0$时，$P(n)$为0. 则对$n\geq 1$，我们有

$$(8)\quad P(n)-P(n-1)-P(n-2)+P(n-5)+P(n-7)+\cdots=0$$

或

$$P(n)=\sum_{k=1}^{\infty}(-1)^{k+1}\{P(n-\omega(k))+P(n-\omega(-k))\}.$$

证明 由定理14.2与定理14.3给出等式

$$\left(1+\sum_{k=1}^{\infty}(-1)^k\{x^{\omega(k)}+x^{\omega(-k)}\}\right)\left(\sum_{m=0}^{\infty}P(m)x^m\right)=1.$$

如果$n\geq 1$，则右端x^n的系数为0，根据系数相等，我们立即得到(8). □

MacMahon利用这个递推公式计算出直到$n=2000$的$P(n)$的值，下面是由他的表中取出的一些有代表性的数值。

$P(1)=1$

$P(5)=7$

$P(10)=42$

$P(15)=176$

$P(20)=627$

$$P(25)=1,958$$
$$P(30)=5,604$$
$$P(40)=37,338$$
$$P(50)=204,226$$
$$P(100)=190,569,292$$
$$P(200)=3,972,999,029,338$$

这些数值说明，$P(n)$随着n迅速地增加．已算出的$P(n)$的最大值是$P(14031)$，它是一个有127位数字的数．D.H.Lehmer[42]算出这个数去证实Ramanujan推测$P(14031)\equiv 0 \pmod{11^4}$，这个推测是正确的．显然，不能用(8)里的递推公式去计算$P(n)$的这个值．作为一个替代的方法，Lehmer利用Rademacher[54]的一个渐近公式去计算它，这个公式是

$$P(n)\sim\frac{e^{k\sqrt{n}}}{4n\sqrt{3}} \quad 当\ n\to\infty时.$$

其中$k=\pi\left(\frac{2}{3}\right)^{\frac{1}{2}}$．对于$n=200$，式中右边的值近似于$4\times 10^{12}$，它非常接近于MacMahon表中给出的$P(200)$的准确的值．

在本书的续集中我们给出$P(n)$的Rademacher渐近公式的来由．这个证明需要相当多的椭圆模函数的予备知识．下一节给出$P(n)$的一个粗略的上界，它包含指数$e^{k\sqrt{n}}$而得到它并非难事．

14.7 $P(n)$的上界

定理14.5 如果$n\geqslant 1$，则有$P(n)\leqslant e^{k\sqrt{n}}$，其中$k=$

$\pi\left(\frac{2}{3}\right)^{\frac{1}{2}}$

证明　令

$$F(x)=\prod_{n=1}^{\infty}(1-x^n)^{-1}=1+\sum_{k=1}^{\infty}P(k)x^k,$$

并限制x在区间$0<x<1$里，于是，我们有$P(n)x^n<F(x)$. 由此得$\log P(n)+n\log x<\log F(x)$，或

$$(9)\quad \log P(n)<\log F(x)+n\log\frac{1}{x}.$$

我们分别估计$\log F(x)$与$n\log\left(\frac{1}{x}\right)$，首先我们写

$$\log F(x)=-\log\prod_{n=1}^{\infty}(1-x^n)=-\sum_{n=1}^{\infty}\log(1-x^n)$$

$$=\sum_{n=1}^{\infty}\sum_{m=1}^{\infty}\frac{x^{mn}}{m}=\sum_{m=1}^{\infty}\frac{1}{m}\sum_{n=1}^{\infty}(x^m)^n$$

$$=\sum_{m=1}^{\infty}\frac{1}{m}\ \frac{x^m}{1-x^m}.$$

因为我们有

$$\frac{1-x^m}{1-x}=1+x+x^2+\cdots+x^{m-1},$$

并因为$0<x<1$，所以我们能写

$$mx^{m-1}<\frac{1-x^m}{1-x}<m,$$

于是

$$\frac{m(1-x)}{x}<\frac{1-x^m}{x^m}<\frac{m(1-x)}{m},$$

颠倒并除以m，得

$$\frac{1}{m^2}\ \frac{x^m}{1-x}\leqslant\frac{1}{m}\ \frac{x^m}{1-x^m}\leqslant\frac{1}{m^2}\ \frac{x}{1-x}.$$

对m求和，我们得

$$\log F(x)=\sum_{m=1}^{\infty}\frac{1}{m}\ \frac{x^m}{1-x^m}\leqslant\frac{x}{1-x}\sum_{m=1}^{\infty}\frac{1}{m^2}$$
$$=\frac{\pi^2}{6}\ \frac{x}{1-x}=\frac{\pi^2}{6t},$$

其中

$$t=\frac{1-x}{x}.$$

注意，当x由0变到1时，t由∞变到0.

下面我们估计$n\log\left(\frac{1}{x}\right)$. 对于$t>0$，我们有$\log(1+t)<t$，但

$$1+t=1+\frac{1-x}{x}=\frac{1}{x}，所以\log\frac{1}{x}<t.$$

于是有

$$(10)\quad \log P(n)<\log F(x)+n\log\frac{1}{x}<\frac{\pi^2}{6t}+nt.$$

$\frac{\pi^2}{6t}+nt$最小值出现在这两项相等时，即$\frac{\pi^2}{6t}=nt$ 或 $t=\frac{\pi}{\sqrt{6n}}$时. 对t的这个值，我们有

$$\log P(n)<2nt=\frac{2n\pi}{\sqrt{6n}}=k\sqrt{n},$$

所以$P(n)<e^{k\sqrt{n}}$，与结论相符. □

注：J.H.van Lint[48]有一个更容易的证明并得到一个更好的不等式

$$(11)\quad P(n)<\frac{\pi e^{k\sqrt{n}}}{\sqrt{6(n-1)}}\quad 对n>1.$$

因为，当$k\geqslant n$时，$P(k)\geqslant P(n)$. 对$n>1$，我们有

$$F(x)>\sum_{k=n}^{\infty}P(k)x^k\geqslant P(n)\sum_{k=n}^{\infty}x^k=\frac{P(n)x^n}{1-x},$$

取对数，我们得到(9)的一个替换不等式

$$\log P(n)<\log F(x)+n\log\frac{1}{x}+\log(1-x).$$

因为$1-x=tx$，我们有$\log(1-x)=\log t-\log\left(\frac{1}{x}\right)$，于是(10)能被

$$(12)\quad \log P(n)<\frac{\pi^2}{6t}+(n-1)t+\log t$$

所代替，容易计算与推导出函数

$$f(t)=\frac{\pi^2}{6t}+(n-1)t+\log t$$

在

$$t=\frac{-1+\sqrt{1+\left[4(n-1)\ \frac{\pi^2}{6}\right]}}{2(n-1)}$$

时有最小值．在(12)里利用t的这个值并去掉不关紧要的项即得(11)．

14.8 Jacobi三重积等式

本节讨论来自theta函数理论的著名的Jacobi等式．Euler五边形数定理与其它许多分拆等式都可视为Jacobi等式的特殊形式．

定理14.8 Jacobi三重积等式．对复数x与z，$|x|<1$，$z\neq0$，我们有

$$(13)\quad \prod_{n=1}^{\infty}(1-x^{2n})(1+x^{2n-1}z^2)(1+x^{2n-1}z^{-2})$$
$$=\sum_{m=-\infty}^{\infty}x^{m^2}z^{2m}.$$

证明　限制$|x|<1$以保证乘积$\Pi(1-x^{2n})$，$\Pi(1+x^{2n-1}z^2)$，$\Pi(1+x^{2n-1}z^{-2})$以及(13)里的级数都绝对收敛．此外，对每一个固定的x，$|x|<1$，级数与这些乘积在不含$z=0$的z平面的紧子集上一致收敛，所以(13)的每一部分是对$z\neq0$的z的解析函数．对于固定的$z\neq0$，这些级数与乘积对$|x|\leqslant r<1$也是一致收敛的，于是表明它们在圆$|x|<1$内是x的解析函数．

为证明(13)，我们保持x固定．对于$z\neq0$，我们用等式

(14) $F(z)=\prod_{n=1}^{\infty}(1+x^{2n-1}z^2)(1+x^{2n-1}z^{-2})$

定义$F(z)$．首先我们指出F满足函数方程

(15) $xz^2F(xz)=F(z)$.

由(14)，得

$$F(xz)=\prod_{n=1}^{\infty}(1+x^{2n+1}z^2)(1+x^{2n-3}z^{-2})$$

$$=\prod_{m=2}^{\infty}(1+x^{2m-1}z^2)\prod_{r=0}^{\infty}(1+x^{2r-1}z^{-2})$$

因为$xz^2=(1+xz^2)(1+x^{-1}z^{-1})$，上面的方程乘以$xz^2$，就得到(15)．

现在令$G(z)$表示(13)左边部分，所以

(16) $G(z)=F(z)\prod_{n=1}^{\infty}(1-x^{2n})$,

于是$G(z)$也满足函数方程(15)．而且，$G(z)$还是z的一个偶函数，它对于所有的$z\neq0$是解析的．所以，它有一个Laurent展式

(17) $G(z)=\sum_{m=-\infty}^{\infty}a_m z^{2m}$,

其中$a_{-m}=a_m$，这因为$G(z)=G(z^{-1})$．（系数a_m依赖于x．）

在(17)里利用函数方程(15)，我们看出系数满足递推公式

$$a_m = x^{2m-1} a_{m-1},$$

多次应用此式，得

$$a_m = a_0 x^{m^2} \quad \text{对所有} m \geqslant 0,$$

因为$1+3+\cdots+(2m-1)=m^2$．上式对$m<0$也成立．于是(17)变为

$$(18)\quad G_x(z)=a_0(x)\sum_{m=-\infty}^{\infty} x^{m^2} z^{2m},$$

其中，我们把$G(z)$写为$G_x(z)$，把a_0写为$a_0(x)$以表示它们对x的依赖于．注意，当$x\to 0$时，(18)式推出$a_0(x)\to 1$．为了完成证明，我们必须证$a_0(x)=1$对所有的x．

在(18)里取$z=e^{\frac{\pi i}{4}}$，得

$$(19)\quad \frac{G_x(e^{\frac{\pi i}{4}})}{a_0(x)}=\sum_{m=-\infty}^{\infty} x^{m^2} i^m=\sum_{n=-\infty}^{\infty}(-1)^n x^{(2n)^2},$$

因为，如果m是奇数，则$i^m=-i^{-m}$．由(18)看出，(19)右端的级数是$\dfrac{G_{x^4}(i)}{a_0(x^4)}$，所以有

$$(20)\quad \frac{G_x(e^{\frac{\pi i}{4}})}{a_0(x)}=\frac{G_{x^4}(i)}{a_0(x^4)}.$$

下面我们证明 $G_x(e^{\frac{\pi i}{4}})=G_{x^4}(i)$．实际上，(14)与(16)给出

$$G_x(e^{\frac{\pi i}{4}})=\prod_{n=1}^{\infty}(1-x^{2n})(1+x^{4n-2}).$$

因为每一个偶数形如$4n$或$4n-2$，所以有

$$\prod_{n=1}^{\infty}(1-x^{2n})=\prod_{n=1}^{\infty}(1-x^{4n})(1-x^{4n-2}),$$

$$G_x(e^{\frac{\pi i}{4}}) = \prod_{n=1}^{\infty}(1-x^{4n})(1-x^{4n-2})(1+x^{4n-2})$$
$$= \prod_{n=1}^{\infty}(1-x^{4n})(1-x^{8n-4})$$
$$= \prod_{n=1}^{\infty}(1-x^{8n})(1-x^{8n-4})(1-x^{8n-4})$$
$$= G_{x^4}(i).$$

于是由(20)得出$a_0(x)=a_0(x^4)$. 再用x^4，x^{4^2}，…代替x，我们得

$$a_0(x)=a_0(x^{4^k}) \quad 对k=1，2，\cdots.$$

但是，当$k\to\infty$时，$x^{4^k}\to 0$. 当$x\to 0$时，$a_0(x)\to 1$. 所以，对所有的x，$a_0(x)=1$. 证明完成. □

14.9 Jacobi等式的推论

在Jacobi等式里，用x^a代替x，用x^b代替z^2，我们得

$$\prod_{n=1}^{\infty}(1-x^{2na})(1+x^{2na-a+b})(1+x^{2na-a-b})$$
$$=\sum_{m=-\infty}^{\infty} x^{am^2+bm}.$$

类似地，当$z^2=-x^b$时，我们得

$$\prod_{n=1}^{\infty}(1-x^{2na})(1-x^{2na-a+b})(1-x^{2na-a-b})$$
$$=\sum_{m=-\infty}^{\infty}(-1)^m x^{am^2+bm}.$$

为得到Euler五边形数定理，在上面最后的等式里取$a=\frac{3}{2}$，$b=\frac{1}{2}$即得.

Jacobi等式导出另一个Euler乘积立方的重要公式。

定理14.7　如果$|x|<1$，则有

$$(21)\quad \prod_{n=1}^{\infty}(1-x^{n})^{3}=\sum_{m=-\infty}^{\infty}(-1)^{m}mx^{\frac{(m^{2}+m)}{2}}$$

$$=\sum_{m=0}^{\infty}(-1)^{m}(2m+1)x^{\frac{(m^{2}+m)}{2}}.$$

证明　在Jacobi等式里用$-xz$代替z^{2}，得

$$\prod_{n=1}^{\infty}(1-x^{2n})(1-x^{2n}z)(1-x^{2n-2}z^{-1})$$

$$=\sum_{m=0}^{\infty}(-1)^{m}x^{m^{2}+m}(z^{m}-z^{-m-1}).$$

现在，我们利用关系式

$$\sum_{n=1}^{\infty}(1-x^{2n-2}z^{-1})=(1-z^{-1})\prod_{n=1}(1-x^{2n}z^{-1})$$

与

$$z^{m}-z^{-m-1}=(1-z^{-1})(1+z^{-1}+z^{-2}+\cdots+z^{-2m})z^{m}$$

重排前式两边的项，并消去因子$1-z^{-1}$，得

$$\prod_{n=1}^{\infty}(1-x^{2n})(1-x^{2n}z)(1-x^{2n}z^{-1})$$

$$=\sum_{m=0}^{\infty}(-1)^{m}x^{m^{2}+m}z^{m}(1+z^{-1}+z^{-2}+\cdots+z^{-2m}).$$

取$z=1$并用$x^{\frac{1}{2}}$代替x，即得(21)。 □

14.10　生成函数的对数微分

定理14.4给出$P(n)$的一个递推公式. 数论函数的递推公式有其它的类型，它能由生成函数的对数微分得到，下面我们叙述这个方法。

令A是一个给定的正整数的集合，并令f(n)是一个给定的数论函数．设乘积

$$F_A(x)=\prod_{n\in A}(1-x^n)^{\frac{-f(n)}{n}}$$

与级数

$$G_A(x)=\sum_{n\in A}\frac{f(n)}{n}x^n$$

对$|x|<1$绝对收敛，并在单位圆内表示解析函数．乘积的对数由

$$\begin{aligned}\log F_A(x)&=-\sum_{n\in A}\frac{f(n)}{n}\log(1-x^n)\\&=\sum_{n\in A}\frac{f(n)}{n}\sum_{m=1}^{\infty}\frac{x^{mn}}{m}\\&=\sum_{m=1}^{\infty}\frac{1}{m}G_A(x^m)\end{aligned}$$

给定．求导数并乘以x，得

$$\begin{aligned}x\frac{F_A'(x)}{F_A(x)}&=\sum_{m=1}^{\infty}G_A'(x^m)x^m=\sum_{m=1}^{\infty}\sum_{n\in A}f(n)x^{mn}\\&=\sum_{m=1}^{\infty}\sum_{n=1}^{\infty}\chi_A(n)f(n)x^{mn},\end{aligned}$$

其中χ_A是集合A的特征函数，

$$\chi_A(n)=\begin{cases}1 & 若n\in A,\\0 & 若n\notin A.\end{cases}$$

把$mn=k$的项集中起来，得

$$\sum_{m=1}^{\infty}\sum_{n=1}^{\infty}\chi_A(n)f(n)x^{mn}=\sum_{k=1}^{\infty}f_A(k)x^k,$$

其中

$$f_A(k)=\sum_{d\mid k}\chi_A(d)f(d)=\sum_{\substack{d\mid k\\d\in A}}f(d).$$

因此我们有下面的等式

$$(22)\quad xF_A'(x)=F_A(x)\sum_{k=1}^{\infty} f_A(k)x^k.$$

把乘积$F_A(x)$写为幂级数

$$F_A(x)=\sum_{n=0}^{\infty} P_{A,f}(n)x^n,\ \text{其中} P_{A,f}(0)=1,$$

在(22)里x^n的系数相等，得到下面定理中的公式(24).

定理14.8　对一个给定的集合A与一个给定的数论函数f，由方程

$$(23)\quad \prod_{n\in A}(1-x^n)^{\frac{-f(n)}{n}}=1+\sum_{n=1}^{\infty} P_{A,f}(n)x^n$$

确定的数$P_{A,f}(n)$满足递推公式

$$(24)\quad nP_{A,f}(n)=\sum_{k=1}^{n} f_A(k)P_{A,f}(n-k),$$

其中$P_{A,f}(0)=1$，且

$$f_A(k)=\sum_{\substack{d\mid k\\ d\in A}} f(d).$$

例 1　令A是全体正整数的集合，如果$f(n)=n$，则$P_{A,f}(n)=P(n)$是自由分拆函数，并且$f_A(k)=\sigma(k)$是k的约数之和. 等式(24)变为

$$nP(n)=\sum_{k=1}^{n}\sigma(k)P(n-k),$$

这是联系乘法数论与加法数论的一个重要的函数关系式.

例 2　取A与例 1 中的 A 相同，但令$f(n)=-n$，则(23)里的系数由Euler五边形数定理确定，而递推公式(24)变为

$$(25)\quad nP_{A,f}(n)=-\sum_{k=1}^{n}\sigma(k)P_{A,f}(n-k)$$

$$= -\sigma(n) - \sum_{k=1}^{n-1} P_{A,f}(k)\sigma(n-k),$$

其中

$$P_{A,f}(n) = \begin{cases} (-1)^m \text{若}n\text{是五边形数}\omega(n)\text{或}\ \omega(-n), \\ 0 \qquad \text{若}n\text{不是五边形数}. \end{cases}$$

(25)也可写为

$$\sigma(n)-\sigma(n-1)-\sigma(n-2)-\sigma(n-5)$$
$$-\sigma(n-7)-\cdots$$
$$= \begin{cases} (-1)^{m-1}\omega(m) & \text{若}n=\omega(m), \\ (-1)^{m-1}\omega(-m) & \text{若}n=\omega(-m), \\ 0 & \text{其它}. \end{cases}$$

当$\sigma(k)$中的$k\leqslant 1$时，左边的和停止．作为说明，当$n=6$与$n=7$时，给出关系式

$$\sigma(6)=\sigma(5)+\sigma(4)-\sigma(1),$$
$$\sigma(7)=\sigma(6)+\sigma(5)-\sigma(2)-7.$$

14.11 Ramanujan的分拆等式

由观察分拆函数的MacMahom 表，Ramanujan 发现了$P(n)$的一些令人惊奇的整除性．例如，他证明了

(26) $P(5m+4)\equiv 0 \pmod{5}$,

(27) $P(7m+5)\equiv 0 \pmod{7}$,

(28) $P(11m+6)\equiv 0 \pmod{11}$.

与此有关，他还宣布了两个当时没有证明的等式

(29) $\sum_{m=0}^{\infty} P(5m+4)x^m = 5\frac{\varphi(x^5)^5}{\varphi(x)^6}$,

$$(30)\quad \sum_{m=0}^{\infty} P(7m+5)x^m = 7\frac{\varphi(x^7)^3}{\varphi(x)^4} + 49x\frac{\varphi(x^7)^7}{\varphi(x)^8},$$

其中

$$\varphi(x) = \prod_{n=1}^{\infty}(1-x^n).$$

因为(29)与(30)右边的函数有整系数的幂级数展开式，所以由Ramanujan等式立即推出(26)与(27).

(29)与(30)的证明是以模函数理论为基础的．这个证明由Dahing, Mordell, Rademacher, Zuckerman 以及其它一些人得到．不依赖于模函数理论的其它的证明由Kruyswijk[36]与后来的Kolberg给出．Kolberg的方法不仅证明了Ramanujan等式而且得到很多新的结果．(29)的 Kruyswijk证明是本章习题11—15的轮廓．

第十四章习题

1． 令A表示正整数的一个非空集合，

(a) 证明乘积

$$\prod_{m\in A}(1-x^m)^{-1}$$

是将n分为部分属于A的分拆数的生成函数．

(b) 描述由乘积

$$\prod_{A\in m}(1+x^m)$$

产生的分拆函数．特别，描述由有限乘积

$\prod_{m=1}^{k}(1+x^m)$产生的分拆函数．

2． 如果$|x|<1$，证明

$$\prod_{n=1}^{\infty}(1+x^{n})=\prod_{m=1}^{\infty}(1-x^{2m-1})^{-1},$$

并推证，n分为不相等部分的分拆数等于n分为奇数个部分的分拆数.

3. 对于复数x与z，$|x|<1$，含

$$f(x,\ z)=\prod_{m=1}^{\infty}(1-x^{m}z).$$

(a) 证明，对每一个固定的x，这个乘积在圆$|x|<1$内是x的解析函数. 并且对每一个固定的x，$|x|<1$，此函数是z的一个整函数.

(b) 由方程

$$f(x,\ z)=\sum_{n=0}^{\infty}a_{n}(x)z^{n}$$

定义数$a_n(x)$. 证明$f(x,\ z)=(1-xz)f(x,\ zx)$并利用此式证明系数满足递推公式

$$a_{n}(x)=a_{n}(x)x^{n}-a_{n-1}(x)x^{n}.$$

(c) 由(b)推出 $a_n(x)=(-1)^n x^{\frac{n(n+1)}{2}}P_n(x)$，其中

$$P_{n}(x)=\prod_{r=1}^{n}(1-x^{r}).$$

这证明下面的等式对$|x|<1$与任意的z成立，

$$\prod_{m=1}^{\infty}(1-x^{m}z)=\prod_{n=0}^{\infty}\frac{(-1)^{n}}{P_{n}(x)}x^{\frac{n(n+1)}{2}}z^{n}.$$

4. 利用与3题类似的方法证明，如果$|x|<1$，$|z|<1$，则有

$$\prod_{m=1}^{\infty}(1-x^{m}z)^{-1}=\sum_{n=0}^{\infty}\frac{z^{n}}{P_{n}(x)},$$

其中 $P_{n}(x)=\prod_{r=1}^{n}(1-x^{r})$.

5. 如果$x \neq 1$，令$\theta_0(x)=1$，并对$n \geqslant 1$，定义

$$\theta_n(x)=\prod_{r=1}^{n} \frac{1-x^{2r}}{1-x^{2r-1}}.$$

(a) 推导出下列Shank有限等式：

$$\sum_{m=1}^{2n} x^{\frac{m(m-1)}{2}}=\sum_{s=0}^{n-1} \frac{\theta_n(x)}{\theta_s(x)} x^{s(2n+1)},$$

$$\sum_{m=1}^{2n+1} x^{\frac{m(m-1)}{2}}=\sum_{s=0}^{n} \frac{\theta_n(x)}{\theta_s(x)} x^{s(2n+1)}.$$

(b) 利用Shank等式推导Gauss三角形数定理

$$\sum_{m=1}^{\infty} x^{\frac{m(m-1)}{2}}=\prod_{n=1}^{\infty} \frac{1-x^{2n}}{1-x^{2n-1}} \quad 对|x|<1.$$

6. 下面的等式对$|x|<1$成立：

$$\sum_{m=-\infty}^{\infty} x^{\frac{m(m+1)}{2}}=\prod_{n=1}^{\infty}(1+x^{n-1})(1-x^{2n}).$$

(a) 由第2题与第5题(b)推出这个等式.

(b) 由Jacbi三重积等式推出这个等式.

7. 证明下列等式对$|x|<1$成立，它们是Jacobi三重积等式的推论：

(a) $$\prod_{n=1}^{\infty}(1-x^{5n})(1-x^{5n-1})(1-x^{5n-4})$$

$$=\sum_{m=-\infty}^{\infty}(-1)^m x^{\frac{m(5m+3)}{2}}.$$

(b) $$\prod_{n=1}^{\infty}(1-x^{5n})(1-x^{5n-2})(1-x^{5n-3})$$

$$=\sum_{m=-\infty}^{\infty}(-1)^m x^{\frac{m(5m+1)}{2}}.$$

8. 证明，14.10节里的递推公式

$$np(n)=\sum_{k=1}^{n} \sigma(k) p(n-k)$$

能表示为

$$np(n)=\sum_{m=1}^{n}\sum_{k\leqslant\frac{n}{m}} mp(n-km).$$

9. 假设每一个正整数K可写为g(k)个不同的形式，这里g(k)是一个正整数.令$p_g(n)$表示n分为部分的分拆的个数,每一个部分K最多出现g(k)个不同的形式. 当g(k)=1时，对所有的K，$p_g(n)$就是自由分拆函数p(n). 找出一个无穷乘积，使它生成$P_g(n)$，并证明有一个数论函数f（依赖于g），使得

$$np_g(n)=\sum_{k=1}^{n} f(k)p_g(n-k).$$

10. 关于14.10节的注释. 由解(22)里的一阶微分方程证明，如果|x|<1，我们有

$$\prod_{n\in A}(1-x^n)^{\frac{-f(n)}{n}}=\exp\left\{\int_0^x\frac{H(t)}{t}dt\right\},$$

其中

$$H(x)=\sum_{k=1}^{\infty} f_A(k)x^k,\quad f_A(k)=\sum_{\substack{d\mid k\\ d\in A}} f(d).$$

并证明

$$\prod_{n=1}^{\infty}(1-x^n)^{\frac{\mu(n)}{n}}=e^{-x}\quad 对|x|<1,$$

其中μ(n)是Möbius函数.

下面各题给出Ramanujan等式

$$\sum_{m=0}^{\infty} p(5m+4)x^m=5\frac{\varphi(x^5)^5}{\varphi(x)^6}$$

其中$\varphi(x)=\prod_{n=1}^{\infty}(1-x^n)$

的证明概要，这个证明用Kruyswijk的方法而不需要模

函数理论.

11. (a) 令$\varepsilon=e^{\frac{2\pi i}{k}}$，$k\geqslant 1$. 证明，对所有的x，我们有

$$\prod_{h=1}^{k}(1-x\varepsilon^{h})=1-x^{k}.$$

(b) 更一般，如果$(n, k)=d$，证明

$$\prod_{h=1}^{k}(1-x\varepsilon^{nh})=(1-x^{\frac{k}{d}})^{d}.$$

并证明

$$\prod_{h=1}^{k}1-x^{n}e^{\frac{2\pi inh}{k}}=\begin{cases}1-x^{nk} & 若(n, k)=1,\\(1-x^{n})^{k} & 若k\mid n.\end{cases}$$

12. (a) 利用11题(b)证明，对素数q与$|x|<1$，我们有

$$\prod_{n=1}^{\infty}\prod_{h=1}^{q}(1-x^{n}e^{\frac{2\pi inh}{q}})=\frac{\varphi(x^{q})^{q+1}}{\varphi(x^{q^{2}})}.$$

(b) 推导出等式

$$\sum_{m=0}^{\infty}p(m)x^{m}=\frac{\varphi(x^{25})}{\varphi(x^{5})^{6}}\prod_{h=1}^{4}\prod_{n=1}^{\infty}(1-x^{n}e^{\frac{2\pi inh}{5}}).$$

13. 如果q是素数且$0\leqslant r<q$，则形如

$$\sum_{n=0}^{\infty}a(n)x^{qn+r}$$

的幂级数称为模q的r型幂级数.

(a) 利用Euler五边形数定理证明$\varphi(x)$是三个幂级数的和，

$$\varphi(x)=\prod_{n=1}^{\infty}(1-x^{n})=I_{0}+I_{1}+I_{2},$$

其中I_{k}表示模5的一个k型幂级数.

(b) 令$\alpha=e^{\frac{2\pi i}{5}}$，证明

$$\prod_{h=1}^{\infty}\prod_{n=1}^{\infty}(1-x^{n}\alpha^{nh})=\prod_{h=1}^{4}(I_{0}+I_{1}\alpha^{h}+I_{2}\alpha^{2h}).$$

(c) 利用12题(b)，证明

$$\sum_{m=0}^{\infty} p(5m+4)x^{5m+4}=V_4\frac{\varphi(x^{25})}{\varphi(x^5)^6},$$

其中V_4是模 5 的一个 4 型幂级数，它由(b)里的乘积得到.

14. (a) 利用定理14.7证明，Euler乘积的立方是三个幂级数的和，

$$\varphi(x)^3=W_0+W_1+W_2,$$

其中W_k表示模 5 的一个K型幂级数.

(b) 利用等式$W_0+W_1+W_2=(I_0+I_1+I_2)^3$证明，13题(a)里的幂级数满足关系式

$$I_0I_2=-I_1^2.$$

(c) 证明$I_1=-x\varphi(x^{25})$.

15. 注意到乘积$\prod_{h=1}^{4}(I_0+I_1\alpha^h+I_\alpha\alpha^{2h})$是次数为 4 的$I_0$，$I_1$，$I_2$的一个齐次多项式，所以由项$I_1^4$，$I_0I_1^2I_2$，$I_0^2I_2^2$给出模 5 的 4 型幂级数的项.

(a) 利用14题(c)证明，存在一个常数c使得

$$V_4=cI_1^4,$$

其中V_4是13题(c)里的幂级数，并推导出

$$\sum_{m=0}^{\infty} p(5m+4)x^{5m+4}=cx^4\frac{\varphi(x^{25})^5}{\varphi(x^5)^6}.$$

(b) 证明$c=5$，并推导出Ramanujan等式

$$\sum_{m=0}^{\infty} p(5m+4)x^m=5\frac{\varphi(x^5)^5}{\varphi(x)^6}.$$

参考文献目录

MR denotes reference to *Mathematical Reviews*.

1. Apostol, Tom M. (1970) Euler's φ-function and separable Gauss sums. *Proc. Amer. Math. Soc*, 24: 482-485; *MR*41, #1661.
2. Apostol, Tom M. (1974) *Mathematical Analysis*, 2nd ed. Reading, Mass.: Addison-Wesley Publishing Co.
3. Ayoub, Raymond G. (1963) *An Introduction to the Analytic Theory of Numbers*. Mathematical Surveys, No. 10. Providence, R.I.: American Mathematical Society.
4. Bell, E. T. (1915) An arithmetical theory of certain numerical functions. *University of Washington Publ. in Math. and Phys. Sci. NO.1, Vol. 1*: 1-44.
5. Borozdkin, K.G. (1956) K voprosu o postoyanni I.M, Vinogradova. *Trudy tretego vsesoiuznogo matematiceskogo siezda, Vol. I*, Moskva [Russian].
6. Buhstab, A.A. (1965) New results in the investigation of the Goldbach-Euler problem and the problem of prime pairs. [Russian]. *Dokl. Akad.*

Nauk SSSR, 162: 735–738; *MR* 31, #2226.[English translation: (1965) *Soviet Math. Dokl*, 6: 729–732.]

7. Chandrasekharan, Komaravolu (1968) *Introduction to Analytic Number Theory*. Die Grundlchren der Mathematischen Wissenschaften, Band 148. New York: Springer–Verlag.
8. Chandrasekharan, Komaravolu (1970) *Arithmetical Functions*. Die Grundlehren der Mathematischen Wissenschaften, Band 167. New York. Springer–Verlag.
9. Chebyshev, P.L. Sur la ionction qui détermine la totalité des nombres premiers inferieurs à une limite donée. (a) (1851) *Mem. Ac. Sc. St. Pétersbourg*, 6: 141–157. (b) (1852) *Jour de Math*(1) 17: 341–365. [*Oeuvres*, 1: 27–48.]
10. Chen, Jing–run (1966) On the representation of a large even integer as the sum of a prime and the product of at most two primes. *Kexue Tongbao* (Foreign Lang. Ed.), 17: 385–386; *MR* 34, #7483.
11. Clarkson, James A.(1966) On the series of prime reciprocals. *Proc. Amer. Math. Soc.*, 17: 541; *MR* 32, #5573.
12. Davenport, Harold (1967) *Multiplicative Number Theory*. Lectures in Advanced Mathematics, No.

1. Chicago: Markham Publishing Co.

13. Dickson, Leonard Eugene (1919) *History of the Theory of Numbers*. (3 volumes). Washington, D. C.: Carnegie Institution of Washington.Reprinted by Chelsea Publishing Co., New York, 1966.

14. Dickson, Leonard Eugene (1930) *Studies in the Theory of Numbers*. Chicago: The University of Chicago Press.

15. Dirichlet, P.G. Lejeune(1837)Beweis des Satzes, dass jede unbegrenzte arithmetische Progression, deren erstes Glied und Differenz ganze Zahlen ohne gemeinschlaftichen Factor sind, unendliche viele Primzahlen enthält. *Abhand. Ak. Wiss. Berlin*: 45-81. [*Werke*, 1: 315-342.]

16. Dirichlet, P.G.Lejeune (1840) Ueber eine Eigenschaft der quadratischen Formen. *Bericht Ak. Wiss. Berlin*: 49-52. [*Werke*, 1: 497-502.]

17. Edwards, H.M. (1974) *Riemann's Zeta Function*. New York and London: Academic Press.

18. Ellison, W.J. (1971) Waring's problem. *Amer. Math. Monthly*, 78: 10-36.

19. Erdös, Paul (1949) On a new method in elementary number theory which leads to an elementary proof. of the prime number theorem. *Proc. Nat. Acad. Sci. U.S.A.*, 35: 374-384: *MR* 10, 595.

20. Euler, Leonhard(1737)Variae observationes circa

series infinitas. *Commentarii Academiae Scientiarum Imperialis Petropolitanae*, 9: 160–188. [*Opera Omnia* (1), 14: 216–244.]

21. Euler, Leonhard (1748) *Introductio in Analysin Infinitorum*, Vol. 1. Lausanne: Bousquet. [*Opera Omnia*(1), 8.]
22. Franklin, F. (1881) Sur le développement du produit infini $(1-x)(1-x^2)(1-x^3)(1-x^4)\cdots$. *Comptes Rendus Acad. Sci. (Paris)*, 92: 448–450.
23. Gauss, C. F. (1801) *Disquisitiones Arithmeticae*. Lipsiae. [English translation: Arthur A. Clarke (1966) New Haven: Yale University Press.
24. Gauss, C.F. (1849) Letter to Encke, dated 24 December. [*Werke*, Vol. II, 444–447.]
25. Gerstenhaber, Murray (1963) The 152nd proof of the law of quadratic reciprocity. *Amer. Math. Monthly*, 70: 397–398; *MR* 27, #100.
26. Goldbach, C. (1742) Letter to Euler, dated 7 June.
27. Grosswald, Emil (1966) *Topics from the Theory of Numbers*. New York: The Macmillan Co.
28. Hadamard, J. (1896) Sur la distribution des zéros de la fonction $\zeta(s)$ et ses conséquences arithmétiques. *Bull. Soc. Math. France*, 24: 199–220.
29. Hagis, Peter, Jr. (1973). A lower bound for the

set of odd perfect numbers. *Math. Comp.*, 27: 951–953; *MR* 48, #3854.

30. Hardy, G. H. (1940) *Ramanujan. Twelve Lectures on Subjects Suggested by His Life and Work*. Cambridge: The University Press.

31. Hardy, G.H. and Wright, E.M. (1960) *An Introduction to the Theory of Numbers*, 4th ed. Oxford: Clarendon Press.

32. Hemer, Ove (1954) Notes on the Diophantine equation $y^2-k=x^3$. *Ark. Mat.*, 3: 67–77; *MR*15, 776.

33. Ingham, A. E. (1932) *The Distribution of Prime Numbers*. Cambridge Tracts in Mathematics and Mathematical Physics, No. 30, Cambridge: The University Press.

34. Jacobi. C.G.J. (1829) *Fundamenta Nova Theoriae Functionum Ellipticarum*. [*Gesammelte Werke*, Band I, 49–239.].

35. Kolesnik, G.A. (1969) An improvement of the remainder term in the divisor problem.(Russian). *Mat. Zametki*, 6: 545–554; *MR*41, #1659. [English translation: (1969), *Math. Notes*, 6: 784–791.]

36. Kruyswijk, D. (1950) On some well-known properties of the partition function $p(n)$ and Euler's infinite product. *Nieuw Arch. Wisk*', (2)23: 97–107; *MR* 11, 715.

37. Landau, E. (1909) *Handbuch der Lehre von der Verteihung der Primzahlen*. Leipzig: Teubner. Reprinted by Chelsea, 1953.
38. Landau, E. (1927) *Vorlesungen* über Zahlentheorie (3 volumes). Leipzig: Hirzel. Reprinted by Chelsea, 1947.
39. Leech, J.(1957)Note on the distribution of prime numbers. *J. London Math. Soc.*, 32: 56–58; *MR* 18, 642.
40. Legendre, A.M. (1798) *Essai sur la Theorie des Nombres*. Paris: Duprat.
41. Lehmer, D. H. (1959) On the exact number of primes less than a given limit. *Illinois J.Math.*, 3: 381–388; *MR* 21, #5613.
42. Lehmer, D.H. (1936) On a conjecture of Ramanujan. *J.London Math . Soc.*, 11: 114–118.
43. Lehmer, D.N. (1914) List of prime numbers from 1 to 10,006,721. Washington, D.C.: Carnegie Institution of Washington, Publ. No. 165.
44. LeVeque, W.J. (1956) *Topics in Number Theory* (2 volumes). Reading, Mass.: Addison–Wesley Publishing Co.
45. LeVeque, W.J. (1974) *Reviews in Number Theory* (6 volumes). Providence, RI: American Mathematical Society.
46. Levinson, N. (1969) A motivated account of an

elementary proof of the prime number theorem. *Amer. Math. Monthly*, 76: 225-245; *MR*39, #2712.

47. Levinson, Norman (1974) More than one third of zeros of Riemann's zeta-function are on $\sigma=1/2$. *Advances Math.*, 13: 383-436.

48. van Lint, Jacobus Hendricus (1974) *Combinatorial Theory Seminar* (Eindhoven University of Technology), Lecture Notes in Mathematics 382. Springer-Verlag, Chapter 4.

49. Littlewood, J.E. (1914) Sur la distribution des nombres premiers. *Comptes Rendus Acad. Sci. (Paris)*, 158: 1869-1872.

50. Mills, W.H. (1947) A prime-representing function. *Bull. Amer. Math. Soc.*, 53: 604; *MR* 8, 567.

51. Nevanlinna, V. (1962) Über den elementaren Beweis des Primzahlsatzes. *Soc. Sci. Fem. Comment. Phys.-Math.*, 27 No. 3, 8 pp.; *MR* 26, #2416.

52. Niven, I. and Zuckerman, H.S. (1972) *An Introduction to the Theory of Numbers*, 3rd ed. New York: John Wiley and Sons, Inc.

53. Prachar, Karl (1957) *Primzahlverteilung*. Die Grundlehren der Mathematischen Wissenschaften, Band 91. Berlin-Göttingen-Heidelberg: Springer-Verlag.

54. Rademacher, Hans (1937) On the partition func-

tion $p(n)$. *proc. London Math. Soc.*, 43: 241-254.

55. Rademacher, Hans (1964) *Lectures on Elementary Number Theory*. New York: Blaisdell Publishing Co.

56. Rademacher, Hans (1973) *Topics in Analytic Number Theory*. Die Grundlehren der Mathematischen Wissenschaften, Band 169.New Yórk-Heidelderg-Berlin: Springer-Verlag.

57. Rényi, A. (1948) On the representation of an even number as the sum of a single prime and a singlc almost-prime number. (Russian). *Izv. Akad. Nauk SSSR Ser. Mat.*, 12: 57-78; *MR* 9, 413. [English translation: (1962) *Amer. Math. Soc. Transl.* 19(2): 299-321.]

58. Riemann, B. (1859) Über die Anzahl der Primzahlen unter einer gegebener Grösse. *Monatsber. Akad. Berlin*. 671-680.

59. Robinson, R.M. (1958) A report on primes of the form $k \cdot 2^n + 1$ and on factors of Fermat numbers. *Proc. Amer. Math. Soc.*, 9: 673-681: *MR* 20, #3097.

60. Rosser, J.Barkley, and Schoenfeld,Lowell(1962) Approximate formulas for some functions of prime number theory. *Illinois J. Math.*, 6: 69-94: *MR* 25. #1139.

61. Schnirelmann, L. (1930) On additive properties

of numbers, (Russian). *Izv. Donskowo Politechn. Inst.* (*Nowostcherkask*), 14(2-3): 3-28.

62. Selberg, Atle (1949) An elementary proof of the prime number theorem. *Ann. of Math.*, 50: 305-313; *MR* 10, 595.

63. Shanks, Daniel (1951) A short proof of an identity of Euler. *Proc. Amer. Math. Soc*, 2: 747-749; *MR* 13, 321.

64. Shapiro, Harold N. (1950) On the number of primes less than or equal x. *Proc. Amer. Math. Soc.*, *1*: 346-348; *MR* 12, 80.

65. Shapiro, Harold N. (1952) On primes in arithmetic progression II. *Ann. of Math*.52: 231-243: *MR* 12, 81.

66. Shen, Mok-Kong (1964) On checking the Goldbach conjecture. *Nordisk Tidskr. Informations-Behandling*, 4: 243-245; *MR* 30, #3051.

67. Sierpiński, Waclaw (1964) *Elementarv Theory of Numbers*. Translated from Polish by A. Hulanicki. Monografie Matematyczne, Tom 42*. warsaw: Państwowe Wzdawnictwo Naukowe.

68. Tatuzawa, Tikao, and Iseki Kaneshiro (1951) On Selberg's elementary proof of the prime number theorem. *Proc. Japan Acad*, 27: 340-342; *MR* 13, 725.

69. Titchmarsh, E.C. (1951) *The Theory of the Riem-*

ann Zeta Function. Oxford: Clarendon Press.

70. Uspensky, J.V., and Heaslett, M.A. (1939) *Elementary Number Theory*. New York: McGraw-Hill Book Co.
71. Vallée Poussin, Ch. de la (1896) Recherches analytiques sur la théorie des nombres premiers. *Ann. Soc. Sci. Bruxelles*, 20_2: 183-256, 281-297.
72. Vinogradov, A.I. (1965) The density hypothesis for Dirichlet *L*-series. (Russian). *Izv. Akad. Nauk SSSR, Ser. Math.* 29: 903-934; *MR* 33, #5579. [Correction: (1966) *ibid.*, 30: 719-720; *MR* 33, #2607.]
73. Vinogradov, I.M. (1937) The representation of an odd number as the sum of three primes. (Russian.) *Dokl. Akad. Nauk SSSR*, 16: 139-142.
74. Vinogradov, I. M. (1954) *Elements of Number Theory*. Translated by S. Kravetz. New York: Dover Publications.
75. Walfisz, A. (1963) *Weylsche Exponentialsummen in der neueren Zahlentheorie*. Mathematische Forschungsberichte, XV, V E B Deutscher Verlag der Wissenschaften, Berlin.
76. Williams, H.C., and Zarnke, C.R. (1972) Some prime numbers of the form $2A3^n+1$ and $2A3^n-1$. *Math. Comp.* 26: 995-998; *MR* 47, #3299.

77. Wrathall, Claude P. (1964) New factors of Fermat numbers. *Math. Comp.*, 18: 324–325; *MR* 29, #1167.

78. Yin, Wen-lin (1956) Note on the representation of large integers as sums of primes. *Bull. Acad. Polon. Sci. Cl. III*, 4: 793–795: *MR* 19, 16.

特殊符号索引

$d\mid n$, $d\nmid n$,	除尽，除不尽，	§1.2
(a, b), $(a_1, \cdots, a_n)$,	最大公约数(gcd)，	§1.2
$[a, b]$,	最小公倍数（lcm），	第一章习题
$\mu(n)$,	Möbius函数，	§2.2
$\varphi(n)$,	Euler函数，	§2.3
$f*g$,	Dirichlet乘积，	§2.6
$I(n)=\left[\frac{1}{n}\right]$,	恒等函数，	§2.6
f^{-1},	Dirichlet逆函数，	§2.7
$u(n)=1$,	单位函数，	§2.7
$\Lambda(n)$,	Mangoldt函数，	§2.8
$\lambda(n)$	Liouville函数，	§2.12
$\sigma_\alpha(n)$, $\sigma(n)$, $d(n)$,	除数函数，	§2.13
$\alpha o F$,	广义卷积，	§2.14
$f_p(x)$,	模P的Bell级数，	§2.16
$f'(n)=f(n)\log n$,	导数，	§2.18
C,	Euler常数，	§3.1
O,	大O符号，	§3.2
$\sim$,	渐近等式，	§3.2
$\zeta(s)$,	Riemann zeta函数，	§3.4
(πx),	$\leqslant x$的素数的个数，	§4.1
$\Psi(x)$,	Chebyshev Ψ—函数，	§4.2
$g(x)$,	Chebyshev g—函数，	§4.2
$M(x)$,	Möbius函数的部分和，	§4.9
o,	小o符号，	§4.9

$a\equiv b \pmod m$,	同余,	§5.1
$\hat{a}$,	剩余类a　modm,	§5.2
a'	a的倒数modm	§5.3
$\chi(n)$,	Dirichlet特征,	§6.8
$L(1,\ \chi)$,	级数$\sum \frac{x(n)}{n}$的和	§6.10
$L'(1,\ \chi)$,	级数$-\sum \frac{x(n)\log n}{n}$的和,	§7.3
$C_k(n)$,	Ramanujan和,	§8.3
$G(n,\ \chi)$,	与x相伴的Gauss和	§8.5
$G(k;\ n)$,	二次Gauss和,	第八章习题
nRp　$n\overline{R}p$,	二次剩余（非剩余）modp,	§9.1
$(n\|p)$,	Legendre符号,	§9.2
$(n\|P)$,	Jacobi符号,	§9.7
$\exp_m(a)$,	a的次数modm,	§10.1
$\mathrm{ind}_g a$,	a的指数以g为底,	§10.10
$L(s,\ \chi)$,	Dirichlet L—函数,	§11.1
σ_a,	绝对收敛横坐标	§11.2
σ_c,	收敛横坐标	§11.6
$\Gamma(s)$,	gamma函数	§12.2
$\zeta(s,\ a)$,	Hurwitz zeta函数	§12.3
$F(x,\ s)$,	周期zeta函数	§12.7
$B_n(x)$, B_n,	Bernoulli多项式，（数）,	§12.11
$\overline{B}_n(x)$,	周期Bernoulli函数,	§12.12
$P(n)$,	分拆函数	§14.1
$\omega(n)$, $\omega(-n)$,	五边形数	§14.4

*　　　*　　　*　　　*　　　*